Opinnäytetyö (AMK)

Tietojenkäsittely

Tietoliikenne

2011

Lillian Jensen, Maire Korpela

TIETOTURVA JA TIETOSUOJA SOSIAALISESSA MEDIASSA

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tietojenkäsittely | Tietoliikenne

Toukokuu 2011 | 57 sivua

Esko Vainikka

Lillian Jensen, Maire Korpela

Tietoturva ja tietosuoja sosiaalisessa mediassa

Sosiaalinen media on tietoverkkoja ja tietotekniikkaa hyödykseen käyttävä viestinnän muoto, jossa tarkoituksena on sisällön tuottaminen vuorovaikutteisesti ja sosiaalisten medioiden avulla luodaan ja ylläpidetään käyttäjien välisiä suhteita. Siihen kuuluu sisältö, yhteisö ja Web 2.0 –teknologia.

Tietoturvalla tarkoitetaan tietojen, palvelujen, järjestelmien ja tietoliikenteen suojaamista. Tietoturva liittyy ulkoisiin tietoturvauhkiin, mutta myös ohjelmointivirheet ovat iso ongelma. Tietoturva seisoo luottamuksellisuuden, eheyden ja käytettävyyden varassa (C-I-A).

Tietosuojassa on kyse siitä, mitä tietoja käyttäjä jakaa itsestään ja kenelle. Rekisterinpitäjän on laadittava kaikista henkilörekistereistä rekisteriseloste ja siitä näkee, kuka käsittelee tietoja ja mihin tarkoitukseen. Lisäksi se sisältää tietoa henkilötietojen suojaamisesta. Tietosuojaan kuuluu C-I-A:n lisäksi pääsynvalvonta sekä kiistämättömyys.

Facebook on maailman suurin ja tunnetuin sosiaalinen media, joka aloitti toimintansa vuonna 2004. Sen pääajatuksena on avoimuus eli Facebookissa on mahdollista pitää yhteyttä ystäviin, jakaa valokuvia, kertoa kiinnostuksen kohteistaan ja toimia muutoinkin aktiivisesti muiden käyttäjien kanssa.

Twitter on perustettu vuonna 2006, mutta sen kävijämäärää on vaikea arvioida, koska yritys ei julkaise aktiivisten tilien määrää. Twitterin päätarkoituksena on käyttäjien päivitysten tekeminen. Siellä käyttäjät voivat lähettää ja lukea toistensa lyhyitä päivityksiä, jotka on rajattu 140 merkkiin.

MySpace on perustettu vuonna 2006 ja vaikka se on edelleen suhteellisen aktiivinen sivusto, sen suosio on tasaisesti laskenut Facebookin lisääntyneen suosion takia. MySpacessa voi muun muassa jakaa musiikkia, kuvia ja videoita sekä pitää blogia.

Sosiaalisessa mediassa, kuten Internetissä muutenkin, on hyvä käyttää arkijärkeä. Ei kannata julkaista mitään, mitä ei ole valmis näyttämään kaikkialle ja kaikille. Liian henkilökohtaisia asioita tai kuvia ei kannata julkaista. Kone kannattaa pitää ajan tasalla sekä yksityisasetukset on myös aina muistettava tarkistaa ennen tietojen lisäämistä. Lisäksi on kunnioitettava muiden yksityisyyttä. Kaikkeen kannattaa suhtautua varauksella.

ASIASANAT: Tietoturva, Tietosuoja, Sosiaalinen media, Facebook, Twitter, MySpace

BACHELOR´S THESIS | ABSTRACT

UNIVERSITY OF APPLIED SCIENCES

Business Information Technology | Data communications

May 2011 | 57 pages

Esko Vainikka

Lillian Jensen, Maire Korpela

Data Privacy and Data Security in Social Media

Social media is a form of communication that uses data networks and communication technology devices. The purpose behind is to interactively produce content and create and maintain social relationships between the users. The three main parts of it are the content, the community and the Web 2.0-technology.

Data security means protecting data, services, systems and data traffic. Data security is connected to external threats, but programming errors are also a big problem. Data security is based on confidentiality, integrity and accessibility (C-I-A).

Data privacy refers to what data you share about yourself and with whom. The maintainer of a user record must make a description of it which shows who administrates and handles the data and for what purpose. In addition, it includes information about protecting personal data. In addition to the C-I-A principles, data privacy also includes access control and indisputability.

Facebook is the largest and best known social media. It started in 2004. The main idea behind it is openness, which means that you can keep in touch with friends, share pictures, talk about your points of interest and interact with other users.

Twitter was founded in 2006. The number of its users is hard to estimate, because Twitter does not release the number of active user accounts. The main purpose of Twitter is sending updates. There users can read and share short updates, that are limited to 140 characters.

MySpace was founded in 2006, and even though it still is a relatively active site, its popularity is steadily declining due to the popularity of Facebook. In MySpace, users can share music, pictures, videos, write a blog and other things.

In social media, as on the Internet in general, it’s good to use common sense. You should not publish anything, which you are not willing to show everyone and everywhere. Topics or pictures that are too personal should not be published. You should also keep your computer updated and always check your privacy settings before you add data. Also, you must respect the privacy of others. Be sure to be cautious towards everything.

KEYWORDS Social Media, Facebook, Twitter, MySpace, Data security, Data privacy

SISÄLTÖ

KUVAT

1 Johdanto

Tämän opinnäytetyön tarkoituksena on selvittää erilaisten sosiaalisten medioiden tietoturvaa ja -suojaa. Erityistä huomiota saavat osakseen tavallisimmat uhkatekijät. Aihetta on lähestytty tavallisen käyttäjän näkökulmasta. Ammattisanastoa on käytetty hyvin vähän, joten asiaan vähemmänkin perehtynyt henkilö kykenee ymmärtämään lukemaansa.

Sosiaalisille medioille, kuten kaikille tietotekniikan osa-alueille, jatkuva kehitys on tyypillinen piirre. Uusia ominaisuuksia, sovelluksia sekä ohjelmia tulee jatkuvasti lisää ja niitä muokataan koko ajan.

Opinnäytetyössä käytetään kvalitatiivista tutkimusotetta. Opinnäytetyössä pyritään kuvaamaan sosiaalisen median tietosuojaa ja –turvaa käytännön kannalta. Aineistoa analysoidaan selityksin ja tekemällä asioista ymmärrettäviä.

Sitä mukaa, kun sosiaalisten medioiden suosio on koko ajan kasvamassa, myös riskien määrä kasvaa. Väärinkäyttäjät ovat erittäin kiinnostuneita pääsemään käsiksi paikkoihin, joissa käyttäjiä on miljoonia, jopa satoja miljoonia, sillä näihin tietoihin käsiksi päästessä liikkuu paljon rahaa.

Tästä syystä on ensiarvoisen tärkeää, että käyttäjät tietävät, mihin he ovat sitoutumassa rekisteröityessään johonkin sosiaaliseen mediaan. On oleellista, että he ymmärtävät tekemistensä mahdolliset seuraukset ja osaavat siksi olla tekemättä näitä virheitä.

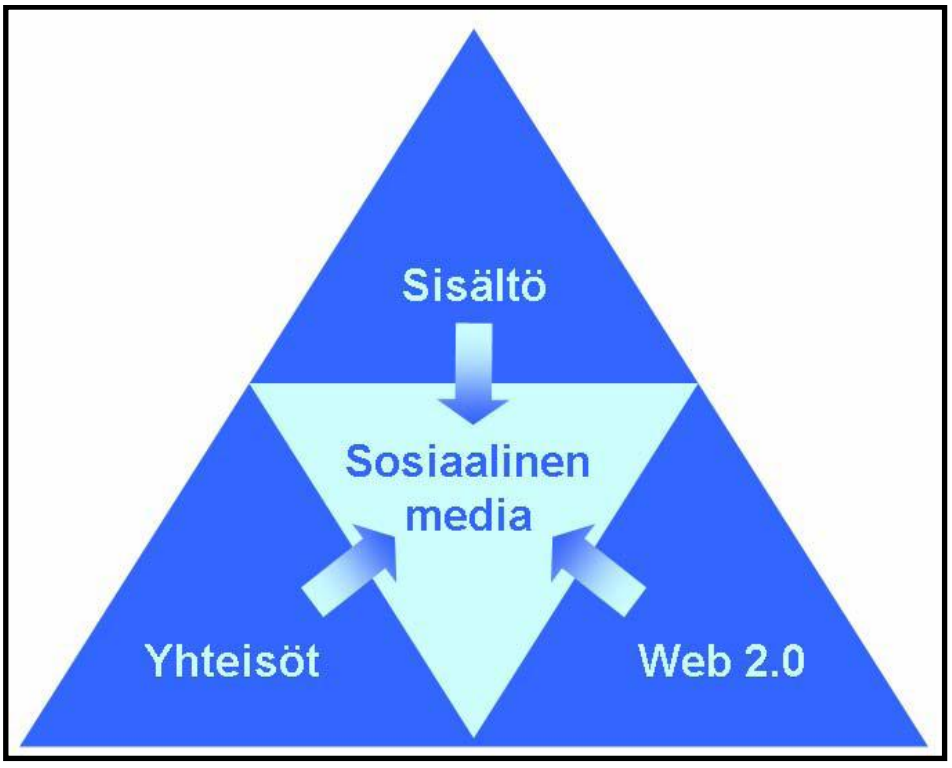
Tässä opinnäytetyössä käsitellään ensin, mitä tarkoittaa sosiaalinen media ja mitä erilaisia osioita siihen kuuluu. Sitten tarkastellaan tietoturvan sekä tietosuojan tarkoitusta. Tämän jälkeen tutustutaan lähemmin joihinkin sosiaalisiin medioihin ja niihin liittyviin ominaisuuksiin. Lopuksi kerrotaan, kuinka kannattaa käyttäytyä sosiaalisessa mediassa mahdollisimman turvallisesti, jotta omat tiedot eivät joudu väärinkäytösten uhriksi, jolloin pahimmassa tapauksessa menettää omaisuutta, rahaa ja maineensa.

2 Sosiaalisen median määrittely

Opinnäytetyön aiheena oleva sosiaalinen media on käsitteenä vielä uusi. Tässä osiossa määritellään sosiaalinen media hieman yksityiskohtaisemmin.

Sosiaalisten medioiden palveluita käyttävät niin yritykset, koulut kuin yhteyshenkilötkin sekä monet muut tahot. Sosiaalisia medioita on useita erilaisia, mutta päätarkoitus niissä on sama eli jakaa kokemuksia toisten käyttäjien kanssa sosiaalisesti. Se on tietoverkkoja ja tietotekniikkaa hyödykseen käyttävä viestinnän muoto, jossa tarkoituksena on sisällön tuottaminen vuorovaikutteisesti ja sosiaalisten medioiden avulla luodaan ja ylläpidetään käyttäjien välisiä suhteita. Käyttäjä voi siis itse tuottaa sisältöä ja viestiä aktiivisesti. (Alanko ym. 2008, 13.)

Sosiaalisen median voidaan ajatella sisältävän kolme elementtiä, jotka ovat sisältö, yhteisö ja Web 2.0 -teknologia (kuva 1) (Kangas ym. 2007, 11).



Kuva 1. Sosiaalisen median koostumus (Kangas ym. 2007, 11).

2.1 Sisältö

Sosiaalisessa mediassa sisällön tuottavat ja jakavat suurimmaksi osaksi käyttäjät. Joukkotiedotusvälineissä ominaista on viestijän ja vastaanottajan välinen kanssakäyminen, kun taas sosiaalisessa mediassa viestintä tapahtuu monelta monelle. Sisältö voi olla uutta, muokattua tai luokiteltua. Uutta sisältöä voivat olla esimerkiksi kuvat, videot, musiikki tai tekstit. Muokattua sisältöä voivat olla muun muassa koosteet ja videoiden miksaus. Luokiteltuun sisältöön kuuluvat esimerkiksi soittolistat, arvostelut ja avainsanat. (Kangas ym. 2007, 13.)

Sosiaalisen median sisällölle ominaisia piirteitä ovat pieni julkaisukynnys, siihen osallistuminen on ilmaista, siellä julkaistu sisältö leviää välittömästi, kukaan ulkopuolinen ei valvo sinne lisättävää sisältöä etukäteen ja se toimii vapaasti hyödynnettävillä alustoilla, joiden ylläpitäjät eivät säätele julkaisutoimintaa perinteisen median keinoin (Tampereen yliopisto 2007).

2.2 Yhteisöt

Yhteisöt muodostuvat yksilöistä, jotka verkostoituvat sosiaalisessa mediassa. Yhteisö voidaan määritellä siten, että sitä käytetään yleisesti ja epätarkasti ryhmämuodostelmien yleisnimityksenä. Käsitteen ala voi vaihdella parista ihmisestä ihmiskuntaan ja alueellinen laajuus voi olla ruokakunnasta koko maapalloon. Käsite viittaa yleensä ihmisten välisen vuorovaikutuksen tapaan, ihmisten väliseen suhteeseen, yhteisyyteen tai siihen, mikä jollekin ihmisryhmälle on yleistä. Yhteisöt voidaan luokitella niiden vuorovaikutuksen luonteen ja tavoitteiden mukaan. (Kangas ym. 2007, 14.)

2.3 Web 2.0

Tim O'Reilly alkoi ensimmäisenä käyttää nimeä Web 2.0 vuonna 2004. Web 2.0 -teknologiassa ei ole kyse mistään Webin toisesta tasosta, vaan pikemminkin uusista ajattelu-, toiminta- ja tuotantotavoista, joita sovelletaan Internet-palvelujen suunnittelussa, ohjelmoinnissa sekä strategiassa. Koko järjestelmän

perustana ovat aktiiviset käyttäjät. Web 2.0 -tekniikat sekä muut ominaisuudet ovat toimineet käytännössä, mikä on lisännyt niiden suosiota. (Hintikka 2007, 6.)

Internet toimii ikään kuin alustana, jossa käyttäjät voivat verkostoitua ja olla yhteydessä keskenään sekä harrastaa muita aktiviteettejä. Web 2.0 -ilmiön määritteleminen on erittäin hankalaa ja monimutkaista, koska siihen kuuluu niin monta uutta ja vanhaa kehityssuuntausta. Sovellusten kannalta Web 2.0 -tekniikassa on hyvänä ominaisuutena se, että se on tarpeeksi muuntautumiskykyinen. Ilmiötä kuvaillaan yleensä siihen liittyvien termien avulla. Muutamia Web 2.0 –teknologiaan liittyviä termejä ovat:

- RSS-syöte
- blogi
- yhteisöllisyys ja käyttäjien luomat sisällöt
- omien sisältöjen ja palveluiden jakaminen maksutta
- ohjelmien ja sovellusten toteuttaminen www-alustalla
- kollektiivinen tuotanto ja kehitys.

(Hintikka 2007, 10.)

3 Tietoturva ja -suoja

Tässä osiossa kerrotaan, mitä tarkoittavat tietoturva sekä tietosuoja. Jotta voidaan ymmärtää, kuinka sosiaalisia medioita voidaan käyttää mahdollisimman turvallisesti, on myös ymmärrettävä, mitä asioita sosiaaliseen mediaan kuuluu. Kun riskit ymmärretään, osataan niihin varautua paremmin ja mahdollisuuksien mukaan estää pahempaa tapahtumasta.

Sosiaaliseen mediaan liittyy lukuisia riskejä. Tällaisia tietoaineistoon liittyviä riskejä ovat muun muassa käyttäjätunnusvarkaudet, identiteettiväärennökset, vakoilu ja tietojen kalastelu. Teknisiä uhkia ovat muun muassa

sovellushaavoittuvuudet, haittaohjelmat ja roskaposti. Lisäksi sosiaalisissa medioissa täytyy jatkuvasti olla ajan tasalla palveluiden kenties epäselvistä ja muuttuvista sopimusehdoista, sillä ylläpitäjillä on oikeus muuttaa niitä haluamaansa muotoon.

3.1 Tietoturva

Tietoturvalla tarkoitetaan tietojen, palvelujen, järjestelmien ja tietoliikenteen suojaamista. Tietoturvassa on olemassa monenlaisia uhkia, joita voivat olla muun muassa erilaiset huijausyritykset, henkilökohtaiset yksityisyyden loukkaukset, roskapostit, teollisuusvakoilut, piratismi ja tietokonevirukset. (Harjuhahto-Madetoja ym. 2006, 19.) Tietoturva liittyy ulkoisiin tietoturvauhkiin eli tahallisesti tehtyihin tietokoneviruksiin, mutta myös tietokoneohjelmien ohjelmointivirheet ovat iso ongelma, sillä ne saattavat aiheuttaa vakaviakin tietoturva-aukkoja, joihin hakkerit pääsevät käsiksi.

Tietoturva seisoo luottamuksellisuuden, eheyden ja käytettävyyden varassa. Kyseessä on kolmijalka, jonka lyhenne on C-I-A (Confidentiality, Integrity, Availability). Luottamuksellisuudella tarkoitetaan tietojen olevan vain niihin oikeutettujen henkilöiden käytössä. Eheydessä tietoja ei ole muutettu, tiedoista ei ole poistettu tai niihin ei ole lisätty mitään ja käytettävyydessä, tai saatavuudessa, tiedot ovat saatavilla oikea-aikaisesti. Näillä kolmella kohdalla ja tietoturvan avulla varmistutaan siitä, että tiedot ovat muuttumattomina vain niihin oikeutettujen henkilöiden käytettävissä ja silloin, kun he niitä tarvitsevat. (Rosendahl 2002.)

Myös ihmisten oma varomattomuus tuo paljon ongelmia, sillä tietokoneen käyttäjät saattavat kielloista huolimatta kirjoittaa salasanojaan ylös ja säilyttää niitä tietokoneen vieressä tai vaikka antaa salasanansa toisen henkilön käyttöön, yleisimmin esimerkiksi puolison. Tästä syystä käyttäjän tiedot voivat helposti päätyä vääriin käsiin luoden tietoturvaongelmia.

Ihmiset myös käyttävät monesti liian helppoja salasanoja kuten vaikka omaa nimeään tai kotipaikkakuntaansa jne. Suositusten mukaan salasanan pitää olla

vähintään 8 merkkiä pitkä ja se sisältää isoja ja pieniä kirjaimia, erikoismerkkejä sekä numeroita sekaisin niiden tarkoittamatta mitään. Lisäksi suosituksena on, että jokaisessa paikassa on eri salasana käytössä ja salasanoja olisi hyvä vaihtaa esimerkiksi kolmen kuukauden välein. (Mediablogi 2008.)

3.2 Tietosuoja

Tietosuojassa on kyse siitä, mitä tietoja käyttäjä jakaa itsestään ja kenelle. Rekisterinpitäjän on laadittava kaikista henkilörekistereistä rekisteriseloste ja käyttäjällä on oikeus pyytää se nähtäväkseen. Rekisteriselosteessa käy ilmi, kuka käsittelee tietoja ja mihin tarkoitukseen. Lisäksi se sisältää tietoa henkilötietojen suojaamisesta. (Tietosuojavaltuutetun toimisto 2011.)

Myös tietosuojaan kuuluu C-I-A, mutta siihen lisätään vielä kaksi osaa, pääsynvalvonta (Access Control) sekä kiistämättömyys (Non-repudiation). Pääsynvalvonnan avulla huolehditaan siitä, että ainoastaan todennetut henkilöt pääsevät käsiksi järjestelmän tietoihin. Kiistämättömyys on tärkeä osa-alue varsinkin sähköisessä kaupankäynnissä ja sillä tarkoitetaan, että asiakas voidaan varmasti todentaa tuotteen tilaajaksi ja myyjä tilauksen vastaanottajaksi ja tuotteen lähettäjäksi. (Rosendahl 2002.)

Tietosuojaperiaatteisiin kuuluu, että käyttäjästä voidaan kerätä tietoa vain hänen suostumuksellaan, siksi joka kerta uudelle sivustolle rekisteröityessä annetaan käyttösopimus luettavaksi ja allekirjoitettavaksi. Käyttäjällä on myös oikeus kieltää tietojen antaminen esimerkiksi suoramarkkinointitarkoitukseen. (Tietosuojavaltuutetun toimisto 2011.)

Lisäksi tietojen keräämisen tulee olla rekisterinpitäjän toiminnan ja tarkoituksen kannalta tarpeellista ja asiallisesti perusteltua sekä tietojen virheettömiä. Kerättyä tietoa ei saa käyttää mihinkään muuhun tarkoitukseen kuin siihen, jota varten ne on kerätty ja arkaluonteista tietoa voidaan kerätä vain henkilötietolaissa säädetyillä erityisillä edellytyksillä. (Tietosuojavaltuutetun toimisto 2011.)

On erittäin tärkeää, että tietoja suojataan, eikä niitä saa luovuttaa ulkopuolisille ilman suostumusta tai luovuttamiseen oikeuttavaa lainsäädäntöä. Yleensä käyttäjällä on oikeus saada tietää henkilötietojen käsittelystä ja oikeus tarkastaa omat tietonsa sekä oikeus vaatia korjausta, jos tiedot ovat virheellisiä. (Tietosuojavaltuutetun toimisto 2011.)

Rekisterinpitäjän on huolehdittava siitä, että käyttäjällä on mahdollisuus saada tieto rekisterinpitäjästä, mihin tarkoitukseen tietoja käytetään ja mihin niitä luovutetaan ja miten voit käyttää oikeuksiasi eli esimerkiksi tarkastusoikeutta ja kielto-oikeutta. Nämä tiedot on kerrottava esimerkiksi silloin, kun tulee asiakkaaksi. Ellet saa tietoja pyytämättä, pitää niitä ehdottomasti pyytää. Jos ei silti saa tietoja, ei sivustolle kannata rekisteröityä ja rekisterinpitäjän on annettava kirjallinen kieltäytymistodistus, jotta asian voi saattaa tietosuojavaltuutetun tutkittavaksi. (Tietosuojavaltuutetun toimisto 2011.)

4 Sosiaalinen media

Opinnäytetyössä käsitellään kolmea tunnettua ja suurta sosiaalista mediaa ja niiden tietoturvaa ja -suojaa. Sosiaaliset mediat on valittu sen mukaan, paljonko sivuilla on käyttäjiä ja siten, että näillä kolmella sivustolla käyttäjät voivat kirjoitella toisilleen ja jakaa kokemuksiaan Tämän perusteella tutkimuskohteeksemme muodostuivat Facebook, MySpace sekä Twitter. Lisäksi nämä kolme sosiaalista mediaa ovat monille tutut varsinkin nimen perusteella.

4.1 Facebook

Facebook on hyvin nopeasti kasvanut yhdeksi maailman suurimmaksi ja tunnetuimmaksi sosiaaliseksi mediaksi. Facebookilla oli rekisteröityneitä käyttäjiä heinäkuussa 2010 jo 500 miljoonaa ja luku kasvaa koko ajan (Zuckerberg 2010). Nykyään käyttäjiä arvioidaan olevan lähemmäs 600 miljoonaa (Social Media 2010). Facebookissa käyttäjät esiintyvät omana itsenään ja sivusto on ilmainen.

Facebook on sosiaalinen media, joka aloitti toimintansa vuonna 2004 Mark Zuckerbergin ja hänen opiskelukavereidensa Eduardo Saverinin, Dustin Moskovitzin ja Chris Hughesin toimesta. Alun perin sivusto oli rajoitettu ainoastaan Harvardin yliopiston opiskelijoille, mutta sen jälkeen sivusto alkoi kattaa muidenkin yliopistojen opiskelijat. Ennen pitkää sivustolle sai rekisteröityä kuka tahansa yli 13-vuotias ja lopulta sivusto laajeni ympäri maailman kaikille halukkaille. (Carlson 2010.)

Facebookissa on mahdollista pitää yhteyttä ystäviin, jakaa valokuvia tai vaikka pelata. Käyttäjä voi omalla sivullaan kertoa kiinnostuksen kohteistaan, status-päivityksessä voi kertoa mitä kuuluu ja voi myös kertoa, missä liikkuu Places-toiminnon avulla. Sivustolla voi lisäksi kommentoida käyttäjien kuvia ja kirjoittaa heidän seinälleen tai yksityisviestejä. Käyttäjä saa itse määritellä, mitä tietoja hän haluaa itsestään julkaista ja kenelle hän haluaa ne näyttää. Facebookissa on paljon tekemistä sen mukaan, mikä itseään kiinnostaa.

Peleissä käyttäjä pelaa tuntemattomien tai ystäviensä kanssa, pelin laadusta riippuen. Peleissä on myös mahdollista käyttää oikeaa rahaa, jonka avulla voi esimerkiksi tehdä pelaamastaan hahmosta hieman paremman. Facebookissa voi myös antaa virtuaalisia lahjoja tai vaikka myydä tavaraa.

Sivustolle lisäämiinsä valokuviin voi merkitä kaverinsa ja Places-toiminnon avulla käyttäjä voi uusimpien puhelinmallien avulla kertoa kartan avulla, missä kulloinkin liikkuu ja he voivat myös kertoa mukana olevista kavereistaan.

Myös monilla yrityksillä on nykyään oma sivu Facebookissa. Sivun avulla he voivat kertoa ajankohtaisista asioista, kuulumisistaan, uusista tarjouksista sekä jakaa vaikka valokuvia näyttääkseen, minkälaista palvelua he tarjoavat. Facebookissa voi myös luoda ja kertoa tapahtumista ja monet yritykset myös järjestävät kilpailuja, joihin voi osallistua vain Facebookin kautta.

4.2 Twitter

Twitter on yhteisöpalvelu, joka on perustettu vuonna 2006 Jack Dorseyn, Evan Williamsin ja Biz Stonen toimesta. Idea sivustoon lähti alun perin kokouksessa,

jossa Dorsey toi esille idean tekstiviestipalvelusta, jonka avulla voitaisiin nopeasti kertoa ryhmässä oleville, mitä kukin sillä hetkellä tekee. Twitter-sanan idea tuli sen tarkoituksesta eli lyhyttä merkityksetöntä tietoa ja ääni, jota linnut tuottavat. (Sagolla 2009.)

Twitterin tarkkaa kävijämäärää on vaikea arvioida, koska yritys ei julkaise aktiivisten tilien määrää. Twitter on kuitenkin listattu maailman yhdeksänneksi suosituimmaksi sivustoksi Alexan analyysin mukaan (Alexa 2011). Käyttäjiä on arvioitu olevan kuukausittain 190 miljoonaa, mutta se ei ole sama asia kuin rekisteröityneiden käyttäjien määrä (Schonfeld 2010).

Twitterin tarkoituksena on käyttäjien päivitysten tekeminen. Twitterissä käyttäjät voivat lähettää ja lukea toistensa lyhyitä päivityksiä, jotka on rajattu 140 merkkiin. Idea on ajalta, jolloin puhelimissa ei ollut vielä yleistä suuret merkkimäärät, joten 140 merkkiä oli loogista. Myös Twitter on ilmainen. Käyttäjien päivityksiä kutsutaan nimellä tweets eli twiitit.

Palvelu on oletuksena kaikille julkinen, mutta profiilinsa voi asettaa yksityiseksi, jolloin vain ystävälistalla olevat henkilöt voivat lukea päivitykset. Twitterissä on mahdollista “seurata” haluamiansa henkilöitä ja sivusto onkin erittäin suosittu julkisuuden henkilöiden keskuudessa.

4.3 MySpace

Kun vuonna 2002 perustettiin Friendster, useat eUniversen työtekijät, joilla oli Friendster-tili, näkivät sivuston potentiaalin ja päättivät kopioida muutamia sivuston suosituimpia ominaisuuksia. Näin syntyi vuonna 2003 MySpace, jonka ensimmäiset käyttäjät olivat eUniversen työntekijät. Tämän jälkeen yritys pisti pystyyn kilpailun, kuka saa sivustolle eniten käyttäjiä. Sitten ei kestänytkään enää kauaa ennen kuin sivustoa tuotiin suurille massoille ja se alkoi kasvaa. (Douglas, 2006.)

MySpace oli pitkään suosituin sosiaalisen median sivusto, mutta sen suosio alkoi laskea sen jälkeen, kun Facebook tuli uusine ominaisuuksineen ja vei MySpacen käyttäjiä. Nykyään MySpacella on 66 miljoonaa käyttäjää, kun pari

vuotta sitten käyttäjiä oli vielä noin 110 miljoonaa. (Owyang 2008.) Toisin kuin Facebookissa, MySpacessa ei tarvitse esiintyä omalla nimellä, vaan sivustolle voi luoda pelkän käyttäjätunnuksen.

MySpacessa käyttäjä voi luoda itselleen profiilin ja ylläpitää blogia. Lisäksi sivustolla voidaan jakaa musiikkia, kuvia ja videoita. Käyttäjät voivat myös itse muokata sivuaan mieleisekseen HTML:n ja CSS:n avulla.

Profiilissaan käyttäjä voi kertoa itsestään muun muassa statuksensa, horoskooppinsa, syntymäaikansa jne. Käyttäjät voivat kommentoida toistensa sivuilla ja he voivat itse poistaa viestejä tai estää viestin julkaisemisen ennen niiden hyväksymistä. MySpacessa käyttäjä voi liittyä erilaisiin ryhmiin tai perustaa oman.

MySpacessa on myös musiikkiosio, joka on hieman erilainen kuin perustili. Musiikkiosiossa artisti voi ladata vaikka kaikki levynsä kuunneltaviksi MP3-versioina. Käyttäjällä täytyy olla oikeus lataamaansa musiikkiin. Lisäksi artistit vailla levy-yhtiötä voivat myydä musiikkiaan sivuston kautta. MySpace on perustanut myös oman levy-yhtiönsä, jonka tarkoituksena on löytää uusia tuntemattomia artisteja.

MySpace tarjoaa lukuisia muitakin käyttömahdollisuuksia kuten kyselyitä, foorumeita tai vaikka karaokea.

MySpacea voi käyttää joko julkisesti tai sen voi muuttaa yksityiseksi. Ikäraja MySpaceen on 13 vuotta ja profiilisivut, joiden käyttäjät merkitsevät iäkseen 13–15 vuotta ovat automaattisesti yksityisiä.

5 Sosiaalisten medioiden tietoturva ja –suoja

Tässä käsitellään kolmea aiemmin mainittua sosiaalista mediaa sekä niihin liittyviä tietoturva- ja suoja-asioita. Facebookin avainajatuksena on avoimuus. Suurin osa tietoturvaongelmista painottuu Facebookiin sen suuren kävijämäärän vuoksi. Tästä syystä Facebookilla on myös muita suurempi osio tässä opinnäytetyössä.

5.1 Facebookin tietoturva ja –suoja

Facebookissa on tällä hetkellä ainakin 500 miljoonaa käyttäjää ja käyttäjien määrä kasvaa jatkuvasti. Siksi on erittäin tärkeää pitää huolta omasta tietoturvastaan ja pitää huolta siitä, etteivät omat tiedot näy kaikille. On tärkeää, että käyttäjät ymmärtävät, mitä tietoja voi näyttää julkisesti ja mitkä tiedot kannattaa ehdottomasti asettaa yksityisiksi. On myös oleellista, että käyttäjät ymmärtävät ja tietävät, mitä tietoja heistä näkyy ja kenelle sekä mitä tietoja heistä jaetaan esimerkiksi kolmansille osapuolille kuten mainostajille.

Tässä osiossa tarkastellaan erilaisia Facebookissa olevia toimintoja ja tutkitaan, mitä ne sisältävät ja kuinka niitä käytetään turvallisemmin. Lisäksi annetaan muutamia esimerkkitapauksia kuinka voi pahimmillaan käydä, jos toimintoja ei osaa käyttää oikeaoppisesti. Facebook on suosituin sosiaalinen media suuren kävijämäärän mukaan. Siitä syystä se on myös suosittu väärinkäyttäjien keskuudessa.

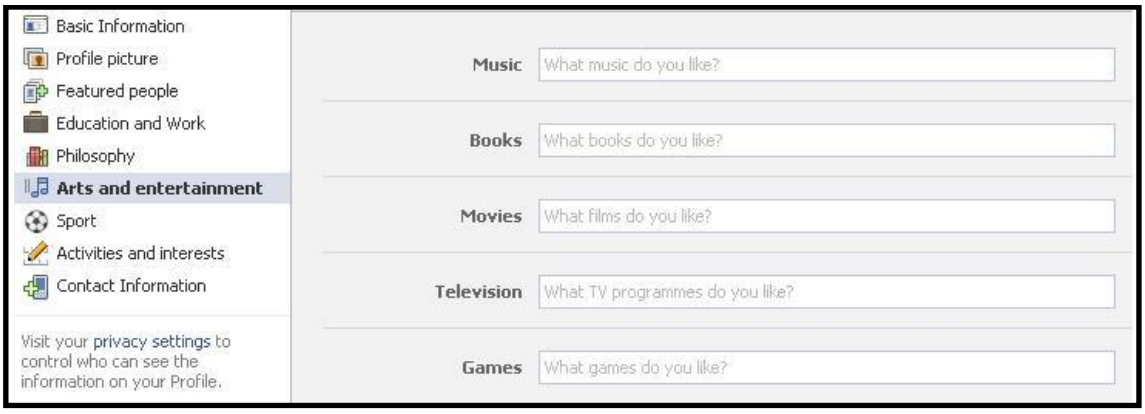
5.1.1 Profiili

Kun käyttäjä rekisteröityy Facebookiin, hän saa käyttäjätilin ja oman profiilin. Aivan kuten missä tahansa muuallakin, uudelle sivustolle rekisteröityessä on tärkeää valita hyvä ja turvallinen salasana. Käyttäjä saa itse päättää, mitä tietoja hän profiiliinsa laittaa. Tällaisia tietoja voivat muun muassa olla profiilikuva, osoite, puhelinnumero ja suhdestatus. Kaikkia tietoja ei tarvitse ilmoittaa, eikä se ole suositeltavaakaan.

Facebookissa alaikärajana on 13 vuotta, mutta siitä huolimatta sivustolle rekisteröityy paljon alaikäisiä, jotka valehtelevat ikänsä. Facebook joutuukin sulkemaan päivittäin yli 20 000 profiilisivua, joista suurin osa kuuluu alle 13-vuotiaille. Tämä tarkoittaakin, että palvelusta poistetaan vuosittain noin seitsemän miljoonaa alaikäistä. Alaikäisyyden lisäksi profiileja suljetaan myös roskapostituksen, sopimattoman sisällön tai muiden palvelun sääntöjen rikkomisten takia. (Pitkänen 2011a.)

Profiilissaan käyttäjä voi myös tarkemmin kertoa erilaisista kiinnostuksenkohteistaan. Kertoa voi muun muassa lempiyhtyeistään, parhaista elokuvista tai harrastuksistaan. Kun kiinnostuksensa kirjoittaa, Facebook tarjoaa automaattisesti erilaisia olemassa olevia ryhmiä, joista käyttäjä kertoo kiinnostuneensa. Näitä ryhmiä voi sitten kuka tahansa tarkastella ja nähdä muita saman kiinnostuksen omaavia ihmisiä. Tämäkin on tuonut ongelmia, sillä Facebookia on ruodittu tavasta, jolla ihmiset kerätään yhteen. Käyttäjät eivät ole innoissaan ajatuksesta, että kaikki Facebookissa olevat näkevät, mistä he ovat kiinnostuneita. Osa käyttäjistä haluaa kiinnostuksen kohteiden näkyvät vain kavereille. Kun kiinnostuksen kohteistaan on kertonut, nämä tahot voivat kertoa käyttäjän etusivulla uusimmista kuulumisista. Esimerkiksi kertoessasi pitäväsi Jenni Vartiaisesta, voi heidän virallinen sivunsa kertoa vaikka uusista keikka-aikatauluista.

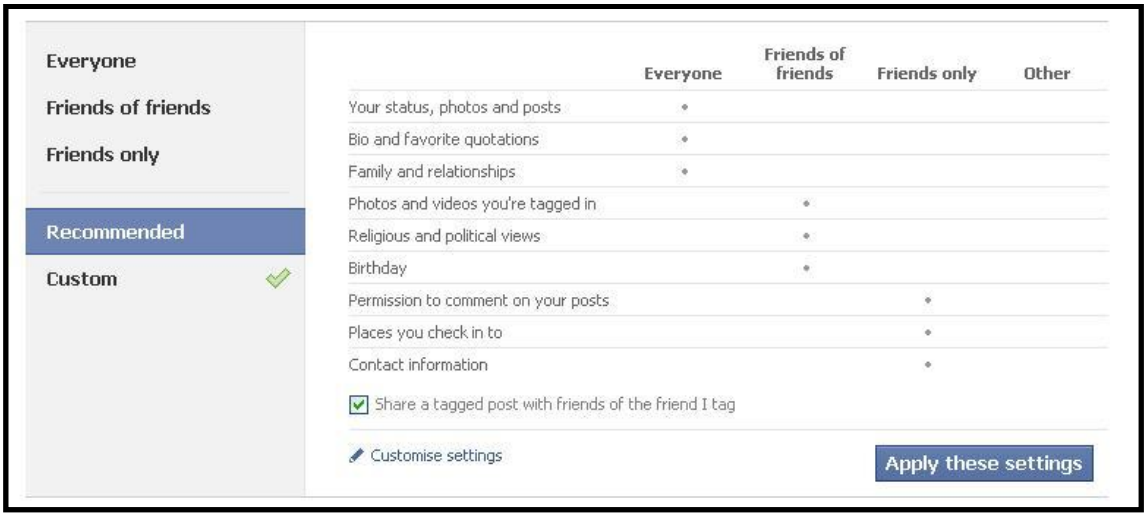
Kuvassa 2 näkyy esimerkkinä, kuinka käyttäjä voi kertoa taiteeseen ja viihteeseen liittyvistä kiinnostuksen kohteistaan. Käyttäjä voi kertoa musiikkiin, kirjoihin, elokuviin, televisio-ohjelmiin sekä peleihin liittyvistä suosikeistaan.



Kuva 2. Kiinnostuksen kohteita.

On suositeltavaa, että ensimmäisiä Facebookissa tehtäviä asioita on oman profiilin yksityiseksi asettaminen. Ei ole suositeltavaa käyttää Facebookin suoraan tarjoamia oletusasetuksia. Varsinkaan, jos käyttäjä julkaisee esimerkiksi sellaisia yksityisiä tietoja itsestään kuin puhelinnumero tai osoite. Kuvassa 3 näkyy, millaisia asetuksia Facebook tarjoaa oletuksena. Kuvat, postaukset ja perhesuhteet esimerkiksi näkyvät kaikille. Merkityt kuvat,

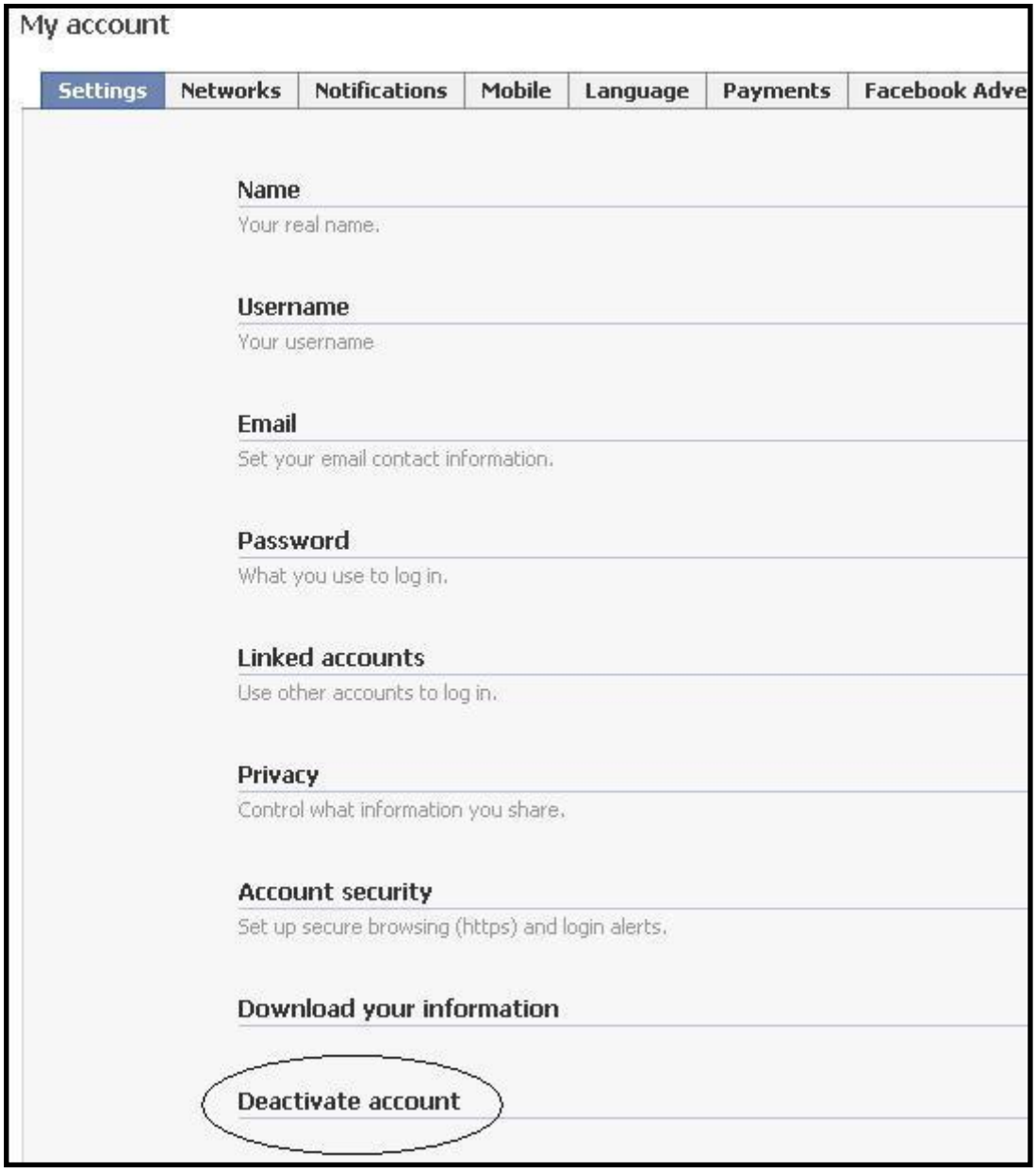
poliittinen vakaumus ja syntymäaika ovat asioita, jotka näytetään kavereiden kavereille ja lupa kommentoinnille ja yhteystiedot näkyvät vain kavereille.



Kuva 3. Facebookin suositusasetukset.

Ammattilaiset suosittelevat, että käyttäjä ei hyväksy mitään tarjottavista asetuksista, vaan tekee kaikki asetukset käsin Custom/Mukautettu-osion kautta. Turvallisinta on laittaa kaikki profiilin tiedot näkymään ainoastaan kavereille. Tällä tavoin ainoastaan kaverit näkevät asiat, jotka olet itsestäsi jakanut sekä valokuvat ja muut mahdolliset toiminnot, jotka profiiliin on lisätty. Nämä tiedot eivät näy edes kavereiden kavereille, eivätkä varsinkaan tuntemattomille. (Pitkänen 2010a.)

Jos käyttäjä haluaa lopettaa Facebookin käytön, se onnistuu käyttäjätilin asetuksista. Siellä on vaihtoehto käyttäjätilin käytön poistamisesta (kuva 4). Tämä toiminto ei kuitenkaan poista tiliä kokonaan, ainoastaan ottaa sen pois käytöstä ja pois näkyvistä. Tällöin käyttäjä poistuu näkyvistä muun muassa ryhmistä ja kaverilistoilta, eikä häntä löydy esimerkiksi Etsi-toiminnon avulla. Tämä johtuu Facebookin mukaan siitä, että käyttäjä saattaa muuttaa myöhemmin mielensä ja haluaakin palata Facebookiin esimerkiksi puolen vuoden päästä. Tällöin käyttäjä voi kirjautua normaalisti sisälle tiliinsä ja kaikki hänen tietonsa säilyvät siellä sinä aikana normaalisti. Käyttäjä on nopeasti takaisin esim. kavereidensa listoilla ja kaikki on taas kuten ennenkin. Facebook pitää kaikki käyttäjän tiedot tallessa poissaoloaikana. (Facebook 2011a.)

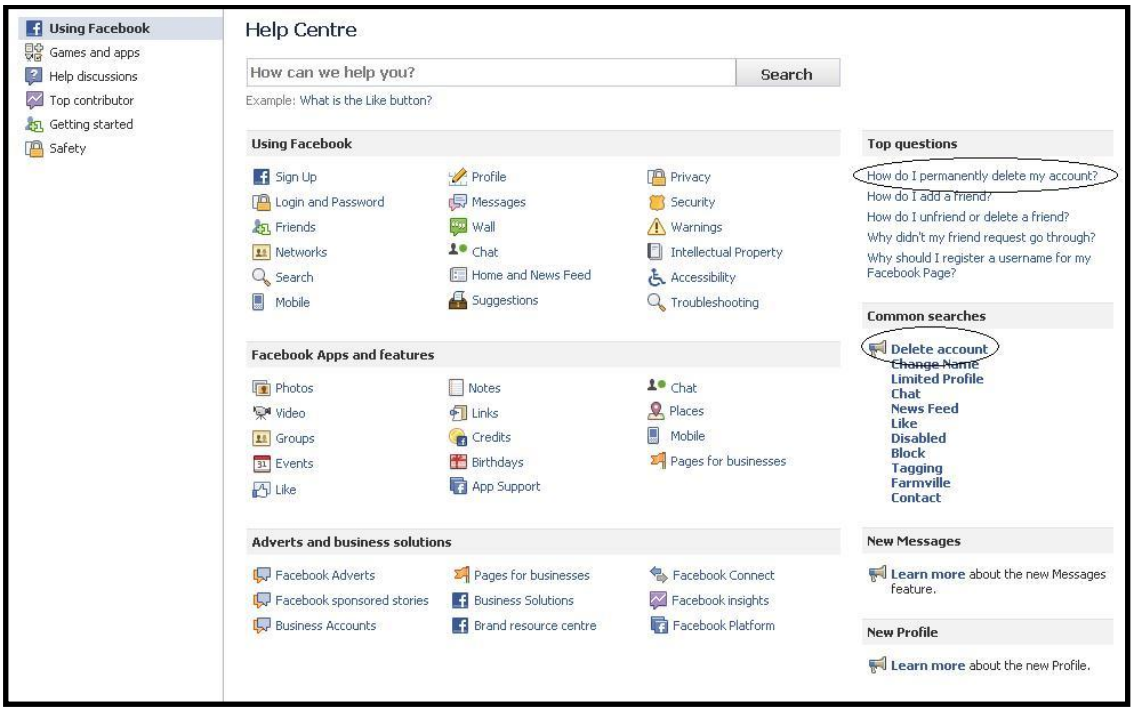


Kuva 4. Käyttäjätilin deaktivointi.

Käyttäjätilin poistaminen kokonaan on vaikeampaa, sillä toiminto on piilotettu monen painalluksen taakse ja sen löytäminen on yllättävän vaikeaa. Esimerkiksi tästä syystä Facebookiin on perustettu ryhmä nimeltä ”How to permanently delete your facebook account”, josta löytyy suoraan linkki sivulle, jossa tilin poistaminen onnistuu. Tilin poistamiseen löytyy kuitenkin apua myös menemällä Help Centreen/Ohje- ja tukikeskukseen Account/Käyttäjätili-palkin kautta (kuva 5).

Kuva 5. Help Centre/Ohje- ja tukikeskus.

Kuvan 6 mukaisesti tukikeskuksen etusivulla on heti kaksi linkkiä, joiden avulla pääsee kokonaan poistamaan tilinsä, jos sitä haluaa.



Kuva 6. Käyttäjätilin poistaminen.

Ongelmana kuitenkin on, että tilin poistamisesta huolimatta käyttäjän tiedot voivat jäädä Facebookin ylläpitäjille. Tästä syystä ryhmän perustaja suositteleekin, että käyttäjän kannattaa ennen lopullista poistoa muun muassa poistaa käsin kaikki tietonsa ja valokuvansa sekä poistaa itsensä kaikista

ryhmistä. Kun tili on kokonaan tyhjä, voi käyttäjä siirtyä poistamaan tilinsä. Tämän jälkeen käyttäjällä on vielä 2 viikkoa aikaa katua valintaansa, mutta jos tiliä ei käytetä kertaakaan seuraavan kahden viikon aikana, tilin pitäisi kokonaan poistua olemasta ja kaikki tiedot sen mukana. (Leijel 2010.)

5.1.2 Kaveripyynnöt

Facebookissa on suosittua kalastella käyttäjän tietoja, koska siellä liikutaan omana itsenä ja yksityisenä henkilönä. Tästä syystä varsinkin aktiivisesti Facebookissa pelaava tai muuten Facebookin palveluja käyttävä voi saada runsaasti kaverikutsuja täysin tuntemattomilta.

On suositeltavaa, että tuntemattomia ei koskaan oteta kavereiksi, koska he pääsevät usein käsiksi kaikkiin tietoihin. Esimerkiksi monet Facebook-pelit kuitenkin ovat sellaisia, ettei kaikkiin ominaisuuksiin pääse käsiksi ilman suurta määrää kavereita, jotka pelaavat samaa peliä. Tästä syystä kavereita on saatava enemmän ja listalle tulee samaa peliä pelaavia henkilöitä, mutta pahimmassa tapauksessa pelaajiksi naamioituneita.

Riippuen, mitä tietoja itsestään on laittanut esille, tuntemattomat voivat päästä käsiksi esimerkiksi sähköpostiosoitteeseen tai puhelinnumeroon, vaikka asetuksista olisikin laitettu ne näkymään vain kavereille, sillä listalle päästyään he ovat ”kavereita”. Täten he voivat levittää saamiaan tietoja ja kuvia hyvinkin laajasti. Lisäksi Facebookissa on mahdollista laittaa asetuksista tiedot näkymään kavereiden kavereille, joten jos käyttäjällä on tämä toiminto päällä ja ystävä on varomaton omien kavereidensa kanssa, tietoihin voivat harmillisesti päästä käsiksi ei-toivotut henkilöt.

Onkin hyvä miettiä, miksi edes haluaisi listalleen tuntemattomia ihmisiä, kyseessä ei kuitenkaan pitäisi olla kisa suosituimmasta henkilöstä. Tuntematon henkilö saattaa olla mukana jonkinlaisessa markkinoinnissa, hän saattaa olla vakooja ja tuntematon henkilö voi saada hyvinkin paljon pahaa aikaiseksi. Ajattelematon kommentti saattaa leviä huomattavasti laajemmalle kuin oli alunperin halunnut aiheuttaen ongelmia. Jotta tietovuodoilta vältyttäisiin, olisi

parasta ottaa kaverikseen vain ihmisiä, jotka oikeasti tuntee ja joiden kanssa on tekemisissä. Vaikka tuntematon olisikin kaveri jonkun käyttäjän ystävän kanssa, se ei tarkoita, että itsekin kannattaisi siitä syystä hyväksyä hänet. (Guyhto 2010.)

5.1.3 Valokuvat

Kun luodaan uusi käyttäjätili, yleensä heti sen jälkeen lisätään profiiliin kuva. Profiilissa on useimmiten käytössä oma kuva, mutta monet laittavat kuvan esimerkiksi lemmikistään tai lapsistaan. Facebookin sivulle käyttäjä voi laittaa valokuvia ja jakaa niitä kavereilleen. Kuvia voi sitten lisätä aina kun siltä tuntuu. Kuvat ovat sikäli riskialttiita, koska kun ne on kerran laitettu Facebookiin, niitä ei saa sieltä enää pois. Jopa jo kertaalleen poistetut kuvat voivat tulla näkyviin joskus myöhemmin, sillä kukaan ei tiedä miten kauan ne säilyvät Facebookin muistissa.

Kaverit voivat halutessaan merkitä käyttäjän omiin kuviinsa. Tästä on kuitenkin aikoinaan tullut lukuisia valituksia, sillä käyttäjä ei voi itse estää merkitsemistään kuviin. Tämä voi olla haitallista varsinkin, jos kyseessä on epäedullinen kuva, esimerkiksi jos oppilaat näkevät kuvan opettajasta vähemmän mairittelevassa valossa. Nykyään merkitystä kuvasta voi kuitenkin itse poistaa merkintänsä. Tällöin kuvaan jää edelleen oma nimi näkyviin, mutta ainakaan se nimi ei enää vie linkillä käyttäjän sivulle. Parasta olisi kuitenkin vain laittaa merkitsijälle viestiä, että poistaa käyttäjän nimen kuvasta kokonaan sekä sopia jo etukäteen kavereiden kanssa, jos ei halua tulla merkityksi kuviin. Tällöin säästytään enemmältä mielipahalta.

Myös kolmas osapuoli voi käyttää kuvia käyttäjää vastaan. Jopa työpaikka voi mennä epäedullisten kuvien vuoksi, mutta sitäkin yleisempää on maineen menetys. Kannattaa olla tarkkana millaisia kuvia itsestään julkaisee. Kannattaa myös estää kavereita julkaisemasta kuviaan, jos haluaa olla aivan varma, ettei mitään pääse läpi ilman hyväksyntää.

Vakuutusyhtiötkin seuraavat sosiaalisten medioiden sivuja saadakseen kiinni petosyritykset. Käyttäjä on esimerkiksi saattanut laittaa valokuvan sivuilleen, jossa hän harrastaa jotain urheilullista, vaikka on juuri työkyvyttömyyden takia hakemassa vakuutuskorvauksia. Tällaisia tapauksia on tullut esille varsin paljon varsinkin Yhdysvalloissa. (Kotilainen 2010.) Toinen huijauksen muoto ovat syrjähypyt, joissa sosiaalisen median kautta paljastetaan puolison uskottomuus.

Nykyisin Facebookissa on käytössä profiilinäkymä, jossa on yläreunassa esillä muutama valokuva käyttäjästä. Kuvat ovat profiilikuvia ja muiden ottamia kuvia, joihin käyttäjä on merkitty. Tämä on tuonut ongelmia, koska kuten aikaisemminkin on mainittu, muiden kuviin merkitseminen voi tarkoittaa epäedullisia kuvia, joita ei halua kaikkien näkevän. Käyttäjä voi kuitenkin estää toisten ottamien valokuvien näkymisen profiilisivullaan joko yksi kerrallaan tai piilottaa ne kaikki. Yksityisyysasetuksia muokkaamalla on mahdollista estää profiilisivultaan kaikki muiden julkaisemat kuvat. (Pitkänen 2011b.)

5.1.4 Paikat/Places

Paikat-toiminto on mahdollinen Facebookin iPhone-sovelluksella sekä muilla kosketusnäyttöpuhelimilla, jotka tukevat html5-standardia ja paikannuspalveluja. Places-toiminnon avulla käyttäjät voivat kertoa Facebookissa, missä he kulloinkin liikkuvat. Käyttäjät voivat ilmoittaa muun muassa missä yökerhossa he ovat julkaisuhetkellä tai vaikka missä he ovat lounastauolla. Palvelua käyttävän tieto ilmestyy oletuksena näkyviin kaikille Facebook-ystäville. (Pitkänen, 2011c.)

Placesin avulla käyttäjät voivat myös kertoa, ketkä heidän kavereistaan ovat menossa mukana. Kaverit saavat kuitenkin ensin ilmoituksen, jossa heidän pitää hyväksyä, että heidänkin olinpaikkansa kerrotaan. Tämä kyselyilmoitus tulee joka kerta uudestaan, kun joku haluaa kertoa käyttäjän sijainnin. Jos ilmoituksen hyväksyy, Facebook olettaa hyväksynnän tarkoittavan kaikkia seuraaviakin kertoja, eikä enää kysy lupaa, vaan julkaisee aina kaverinkin sijainnin käyttäjän niin tehdessä. Käyttäjän on kuitenkin asetusten kautta mahdollista estää koko Places-toiminto, jolloin kukaan käyttäjän kavereista ei

voi enää kertoa käyttäjän sijaintia. Jos kuitenkin haluaa poistaa itsensä kavereiden Paikat-päivityksistä, se onnistuu myös jälkeenpäin. (Pitkänen 2011c.)

Places on myös tuottanut ongelmia sen julkaisusta lähtien. Yksityisyyden suojastaan tarkat eivät pidä siitä, että kerran julkaisun hyväksyttyään Facebook antaa tulevaisuudessa aina luvan julkaista käyttäjän sijainnin. Lisäksi toiminto on antanut murtovarkaille oivan tavan seurata milloin ihmiset ovat poissa kotoaan. Kaikki eivät ymmärrä laittaa profiiliaan tarpeeksi salaisiksi, jolloin kaikki seinällä julkaistavat tiedot näkyvät kaikille. Tästä syystä varkaiden on helppo seurata ihmisten tekemisiä ja jopa selvittää asuinsijainti esimerkiksi valokuvien tai seinäkirjoitusten perusteella. Kun Places kertoo käyttäjän olevan poissa koko yön, varkaat voivat mennä tämän kotiin ja ryöstää sen. (Pitkänen 2011c.)

Places-asetuksiin pääsee käsiksi Privacy Settings/Yksityisyysasetukset - napin kautta yläoikealta. Alhaalta löytyy Customise settings/Mukautetut asetukset - nappi, jota painamalla pääsee lisäasetuksiin käsiksi. Seuraavaksi aukeavalla sivulla käyttäjä voi päättää muun muassa, voivatko kaverit merkitä käyttäjän seuralaiseksi paikkoihin (kuvat 7 ja 8).

Kuva 7. Kenelle paikkoihin meneminen näkyy.

Kuva 8. Kavereiden mahdollisuus merkitä paikkoihin.

5.1.5 Linkit

Facebookissa linkit näkyvät sivun Uutiset-otsikon alapuolelta, mutta niitä voi liikkua myös chatin kautta. Linkkejä voidaan, aivan kuten muitakin uutisia,

jakaa, kommentoida tai tykätä tai kaikkia näitä. Aika usein linkki voi olla esimerkiksi YouTubesta ladattu musiikkivideo, jota sitten jaetaan kavereille. Linkin avulla pääset siirtymään jollekin toiselle sivulle tai sivustolle. Tähän liittyy tietysti vaaransa, koska linkki voikin olla sivulle, jossa on mato tai jokin muu haittaohjelma. Yleensä mitä houkuttelevampi linkki on, sitä varmemmin se on haittaohjelma kuten mato.

Ensimmäinen suomenkielinen mato levisi Facebookiin lokakuussa 2010. Tykkääjiä oli yli 106 000. Kyseessä on click-jacking tyyppinen huijaus, jota käytetään paljon. Huijauksessa uhrit todellisuudessa suosittelevat linkkiä ystävilleen, vaikka luulevat tekevänsä jotain muuta. Linkin otsikko voi olla ” Voi paska, katso miten kävi kun isä näki tyttärensä webcam-esityksen.” (Pitkänen 2010b.)

Linkin avaaja joutuu sivulle, missä häntä varoitetaan sisällöstä, joka voi järkyttää häntä. Seuraavalla sivulla avaajaa pyydetään painamaan numeroita 1, 2 ja 3 ja numeroiden painaminen näkyy ystäville ”tykkäämisenä”. Kaverit saattavat myös kiinnostua linkin sisällöstä ja painavat linkkiä, jolloin kierre jatkuu. Seuraavakaan sivu ei välttämättä näytä luvattua sisältöä, vaan saattaa tarjota mahdollisuuden voittaa tavaroita, jos linkin avaaja antaa puhelinnumeronsa. Annettuaan puhelinnumeronsa huijarit voivat vaikka periä tietyn summan kuukaudessa puhelinlaskulla. Puhelinnumeron antamisen jälkeen linkki näyttää vihdoin kaivatun sisällön. Useimmiten saman videon näkeminen on huomattavasti helpompaa sekä myös ilmaista, kun menee suoraan YouTuben sivulle etsimään videon. (Pitkänen 2010b.)

Muutama päivä tapauksen jälkeen julkaistiin tieto, jossa kerrottiin, että huijauksen uhreiksi joutuneet eivät joudu maksamaan mitään mobiilisisältöä, jonka he tahtomattaan latasivat (Linnake 2010c). Tällaisia click-jacking -huijauksia on ollut liikkeellä useita, muun muassa Lady Gaga –huijaus, maailman kuumimmat naiset ja Paramoren alastonkuvat.

Facebookissa itsessään ei ole automaattista suodatusta haittaohjelmien varalle, joten se on oivallinen kohde hyökkäysten tekijöille. Toinen houkutteleva tekijä

on mahdollisuus käyttää lyhennettyjä linkkejä, joista ei voi ennalta aavistaa linkin sisältöä.

On hyvä pitää mielessä, että kaikkia linkkejä ei kannata painaa. Jo se, että linkki tulee tutulta kaverilta, tekee linkistä houkuttelevan ja luo väärää turvallisuuden tunnetta. Jos ei ole täysin varma linkin turvallisuudesta, sen painamisen sijaan suositellaan kysymään suoraan lähettäjältä, mistä linkissä on kyse. Tämä ei ole suurikaan vaiva verrattaessa siihen, mitä olisi voinut tapahtua pahimmassa tapauksessa: menettää koneen hallinnan jollekin toiselle ja rahat myös. (Facebook 2011b.)

5.1.6 Ryhmät ja sovellukset

Ryhmät toiminto oli Facebookissa pitkään käytössä aktiivisesti, mutta sitten se otettiin ikään kuin pois käytöstä joksikin aikaa ja syksyllä 2010 se tuli takaisin uudistettuna. Facebook on täynnä ryhmiä, joista voi joko tykätä tai niihin voi liittyä mukaan. On myös mahdollista itse perustaa ryhmiä ja tehdä niistä joko julkisia tai yksityisiä ja Facebookin käyttäjiä voi lokeroida kaveriporukoitaan osiin ja kommunikoida vain valittujen henkilöiden kanssa. Ryhmät ovat oletuksena suljettuja. (Linnake 2010a.)

Facebookin uudistetut ryhmäsivut toivat kuitenkin heti alussa suuriakin ongelmia. Jos yksikin käyttäjä kaveripiiristä oli jossain ryhmässä mukana, pystyi hän lisäämään kenet tahansa kavereistaan mukaan ryhmään tämän haluamatta. Tämä ongelma tuli julkisuuteen, kun muun muassa Facebookin perustaja Mark Zuckerberg löysi itsensä NAMBLA-nimisestä ryhmästä, jonka voi liittää pedofiliaan. NAMBLA voi tarkoittaa South Parkiin liittyen joko Marlon Brando –kaksoisolentojen kansallista järjestöä tai Pohjois-Amerikan mies- ja poikarakkausjärjestöä. Ihmisten lisäämistä kavereiden ryhmiin ei voida estää, eikä ryhmästä voi poistua kuin jälkikäteen. Ainoa mitä käyttäjä voi tehdä, on kieltää kavereita tekemästä näin tai estää tai poistaa heidät kaverilistalta kokonaan. (Uusi Facebook-toiminto nosti myrskyn 2010 ; Linnake 2010b.)

Lisäksi Facebookissa on paljon yrityksiin liittyviä ryhmiä sekä sovelluksia. Vaikka niistä moni onkin aitoja, myös paljon huijausyrityksiä on liikenteessä. Tällaisissa ryhmissä on esimerkiksi mahdollista osallistua kilpailuihin voittaakseen lahjakortteja ja niihin osallistuakseen on annettava muun muassa puhelinnumerotietonsa sekä sähköpostitietonsa, jopa henkilötunnuksensa. Lisäksi kriteerinä saattaa olla, että kavereita pitää kutsua tietty määrä mukaan. (Digitoday 2010.)

Aina tietoja ei edes tarvitse antaa, sillä Facebookissa alkaessa käyttää mitä tahansa sovellusta, liityttäessä kysytään käyttäjältä lupa siihen, että sovellus saa käyttää tämän tietoja. Käyttäjät eivät välttämättä katso kovin tarkkaan, mihin ovat liittymässä, vaan valitsevat suoraan vaihtoehdon salli. Vaikka sovellus pääsee käsiksi vain tietoihin, jotka käyttäjä on muutenkin asettanut julkisiksi, on niiden leviäminen laajemmin todennäköisempää, jos sovellukselle annetaan suoraan oikeus päästä käsiksi profiiliin kuten esimerkiksi profiilikuvaan ja syntymäaikaan.

Hyvänä esimerkkinä voidaan antaa esimerkiksi treffipalvelu nimeltä Badoo. Palvelu käytti kuitenkin luvatonta tietojen kalastelua Facebookissa. Badoon sovellukset olivat yhteydessä palveluun ja käyttäjän alkaessa käyttää sitä ja antaessaan luvan tietojensa käyttöön, siirtyi hänen tietonsa välittömästi myös Badoon sivulle seuranhakuilmoituksena. Sen lisäksi, että sovellus keräsi tietoja käyttäjästä, se teki sitä myös käyttäjän ystävistä. Käyttäjälle ei kerrota tietojen käytöstä palvelussa. (Reinikainen 2011.)

5.1.7 Pelit

Facebookissa on paljon tarjolla erilaisia pelejä. Pelit perustuvat kahteen eri logiikkaan. Pelaaja voi joko kerätä tarpeeksi pisteitä päästäkseen seuraavalle tasolle tai pelaajalla voi olla käytettävänään tietty määrä energiaa, jonka loputtua ei voi pelata ennen kuin se ajan myötä taas lisääntyy.

Monissa peleissä on ajatuksena, että mitä enemmän kavereita, sen parempi, koska silloin pelaaja saa kaikki pelin edut käyttöönsä. Tällaisia etuja voi olla esimerkiksi jonkin tehtävän suorittaminen, joka ei muuten onnistuisi.

Facebookiin voidaan luoda pelien omia ryhmiä, joita kolmas osapuoli, kuten mainostajat, voivat käyttää hyväkseen. Ryhmien avulla käyttäjä voi saada uusia kavereita perustuen siihen, että he pelaavat samaa peliä, mitään muuta tietoa käyttäjällä ei välttämättä ”uudesta kaveristaan” sitten olekaan. Tällä tavalla lisätty kaveri on aina turvallisuusriski, jos käyttäjä ei ymmärrä muokata profiilinsa asetuksia. Siksi olisi tärkeää laittaa esimerkiksi kaksi erilaista kaverilistaa. Toisessa ovat oikeat kaverit ja toisessa pelikaverit. Toinen ryhmä näkee kaikki tiedot ja kuvat, mutta pelaavat sekä tuntemattomat kaverit eivät näe mitään, heidän kanssaan voi vain pelata, kuten on alun perin ollut tarkoituskin.

Peleissä voidaan käyttää oikeaa rahaa ostamalla pelimerkkejä peleihin, joilla taas voidaan ostaa erilaisia tuotteita. Käytettäessä oikeaa rahaa pelaajan on käytävä omassa pankissa ja tehtävä tilisiirto. Tämä toiminto voi olla tietoturvariski. Joku toinen osapuoli voi päästä tietoihin käsiksi, jos pelaaja käyttää yleistä tietokonetta tai julkisen tilan wlan-verkkoa. Monissa peleissä on myös saatavilla rahallisia pelikortteja, jotka toimivat prepaid-tyyliin, mutta tätä mahdollisuutta ei ainakaan vielä ole Suomessa (Vääräniemi 2010).

Krediitti on Facebookin virtuaalivaluutta, jolla voi ostaa moniin peleihin pelien omaa valuuttaa tai tavaroita. Halutessaan lisää krediittiä, voi sen hankkimiseen käyttää tavallisia maksuvälineitä kuten erilaisia pankki- ja luottokortteja. Maksettaessa on syytä noudattaa yleistä varovaisuutta ottamalla huomioon erilaiset riskitekijät, jotka liittyvät rahan käyttöön Internetissä.

Pelit ovat suosittu sovellus sosiaalisessa mediassa. Siihen kohdistuvia tietoturva- tai tietosuojatapauksia on käyttäjäkuntaan nähden varsin vähän. Muutamia hyökkäyksiä on ollut, mutta niistä ei ole julkisuudessa paljon tietoa. Otaksuttavasti tietoturvaan liittyvät riskit peleissä ovat vasta tulevaisuuden asioita.

5.1.8 Väliaikainen salasana

Facebookissa on myös käytössä 20 minuutin kertakäyttöinen salasana. Suomessa palvelu ei kuitenkaan ole käytössä, vaan ainoastaan Yhdysvalloissa.

Monet käyttävät Facebookia ja muitakin sosiaalisia medioita julkisissa koneissa ja tästä syystä Facebook toi markkinoille kertakäyttösalasanoja. Käyttäjä voi, halutessaan päästä Facebookiin, lähettää puhelimestaan otp (one time password)-tekstiviestin, jolloin hän saa tekstiviestinä takaisin väliaikaisen salasanan. Salasana on voimassa 20 minuuttia sen jälkeen, kun sen on saanut. Palvelun käyttäminen edellyttää, että Facebookilla on tieto käyttäjän matkapuhelinnumerosta. (Vaalisto 2010.)

Toiminto on ajankohtainen siitä syystä, ettei koskaan voi tietää, kuka julkisissa paikoissa katselee koneen käyttöä tai mitä tietoja koneelle jää ja kuka tulee käyttämään konetta jälkeenpäin. Yleisiä wlan-verkkoja käyttäessä on aina olemassa omat riskinsä.

Toimintoa on kuitenkin kritisoitu siitä, että se luottaa liikaa käyttäjäänsä. Jos joku ulkopuolinen saa puhelimen käyttöönsä omistajan kadottaessa puhelimensa, vahingontekijä voi lähettää viestin ja saadessaan väliaikaisen salasanan, käydä muokkaamassa tilin asetuksia ja ottaa sen sitten kokonaan käyttöönsä. Lisäksi ongelmana voi olla, etteivät käyttäjät välttämättä edes huomaa, vaikka ulkopuolinen olisi muuttanut tiliin liitetyn matkapuhelinnumeron tietoja omikseen. Tämä onnistuu vaikka silloin, kun kirjautunut käyttäjä päättää käydä nopeasti vaikka vessassa. Lisäksi on otettu esille, miksi pitäisi julkisesti edes käyttää Facebookia, jos ei ole varma sen turvallisuudesta. (Linnake 2010d.)

Arvostelijoilla on kuitenkin myös hyvää sanottavaa, sillä esimerkiksi näppäinten painalluksia tallentavat haittaohjelmat eivät hyödy väliaikaisesta salasanasta, koska se muuttuu kuitenkin nopeasti toimimattomaksi (Linnake 2010d).

5.1.9 Viestit

Viestejä voi lähettää yhdelle tai useammalle kaverille, eivätkä ne näy muille kuin niille, joille se on lähetetty. Niitä voi kirjoittaa myös seinälle ja asetuksista voi säätää kenelle seinälle kirjoitetut viestit näkyvät.

Kun viestejä kirjoittaa seinälle, kannattaa miettiä tarkkaan, mitä on tekemässä. Esimerkiksi tulevista matkoista ei kannata mainita mitään ennen kuin vasta matkan jälkeen. Ei myöskään kannata mainita mitään siitä, kuinka paljon on huijannut verottajaa tai vakuutusyhtiötä.

Työnantajan haukkuminen ei myöskään ole suotavaa Facebookissa. Sen seurauksena monet ovat menettäneet työpaikkansa, myös Suomessa tällaisia tapauksia on tullut julki. Yksi esimerkki kertoo brittiläisestä naisesta, joka haukkui esimiestään törkeästi, eikä ollut muistanut, että myös tämä oli hänen kaverilistallaan, ennen kuin asiasta huomautettiin, esimiehen toimesta. Esimies ilmoittikin samaisessa viestissä, että kahden viikon koeajan jälkeen työntekijän ei tarvinnut enää tulla takaisin töihin. (Koskinen 2011, 2.)

5.1.10 HTTPS

Facebookissa on nykyään tarjolla sivuston käyttäminen salatussa eli HTTPS-muodossa. Aikaisemmin kaikki tiedot lähetettiin salaamattomana liikenteenä, joten periaatteessa kuka tahansa saattoi nähdä lähetetyt tiedot ja päästä niihin käsiksi. Ongelma on suuri varsinkin julkisia koneita käyttäessä, koska niiden suojauksista ei voi olla varmuutta, niihin pääsee kuka tahansa käsiksi, eivätkä kaikki osaa peittää jälkiänsä esimerkiksi poistamalla evästeitä koneen käytön jälkeen.

Tästä syystä Facebook tarjoaa mahdollisuuden käyttää salattua lähetysmenetelmää. Menetelmä ei ole kuitenkaan oletuksena käytössä, vaan käyttäjän pitää itse mennä muuttamaan se asetuksista. Facebook kertoo asetuksissaan, että salattua menetelmää käytetään aina kuin mahdollista. Kaikki Facebookissa olevat palvelut eivät esimerkiksi tue HTTPS-toimintoa, vaan käyttäjän on palattava normaaliin http-yhteyteen ennen kuin voi siirtyä

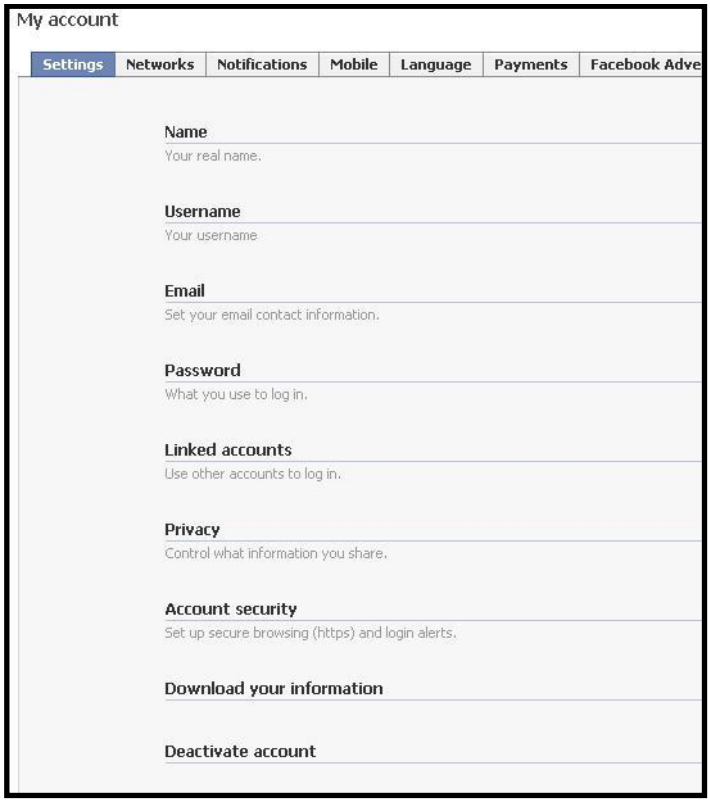
palveluntarjoajan sivulle. Ongelmana kuitenkin on, että kun palvelusta poistuu, Facebook ei palaa HTTPS-muotoon, vaan se pitää jälleen mennä laittamaan käsin päälle. (Linnake 2011.) Facebook on kuitenkin huomioinut ongelman ja nykyään HTTPS palautuu automaattisesti, kun käyttäjä poistuu palvelusta ja kirjautuu takaisin sisälle.

Facebook on lisäksi alkanut tarjota mahdollisuutta saada sähköposti-ilmoituksen aina, kun vieras kone kirjautuu käyttäjän tilille ja onkin erittäin suositeltavaa ottaa toiminto käyttöön. Myös tämä onnistuu käyttäjän yksityisasetusten kautta. Omalla kotikoneellaan kirjautuessa voi laittaa rastin ruutuun, ettei koneen nimeämistä enää kysytä, jos ei halua joka kerta antaa koneelle nimeä kirjautuessaan sisälle. Kuitenkin joka kerta, kun tilille kirjautuu joku eri koneelta, tulee siitä välittömästi sähköpostia käyttäjälle. Jos käyttäjä ei ole itse kirjautunut vieraalta koneelta, sähköposti tarjoaa linkkiä asian ilmoittamisesta, jolloin esimerkiksi väärinkäyttäjän muuttamat tiedot eivät tule voimaan ja hänet saadaan potkaistua ulos käyttäjän tililtä.

Käyttäjä pääsee asetuksiin käsiksi Account Settingsin/Käyttäjätilin asetukset -kautta (kuva 9).

Kuva 9. Käyttäjätilin asetukset.

Asetukset näkyvät jo heti ensimmäisellä sivulla (kuva 10).



Kuva 10. Asetusten etusivu.

Valitsemalla Account Securityn/Käyttäjätilin turvallisuus pääsee muokkaamaan salattua yhteyttä ja asettamaan sähköpostiinsa tulemaan ilmoituksia, kun tiliä käytetään joltain uudelta koneelta (kuva 11).

Kuva 11. HTTPS sekä uusi tietokone –asetukset.

5.2 Twitterin tietoturva ja –suoja

Toisin kuin Facebookissa, Twitterissä käyttäjätilit ovat pääosin julkisia. Twitterissä käyttäjät voivat seurata haluamiansa henkilöitä ja kuka tahansa voi seurata käyttäjää. Julkisen muotonsa takia Twitterissä ei tarvitse samalla tavalla miettiä yksityisyyden suojaansa tai yksityisiä asetuksiaan, koska käyttötarkoituksena on kaiken näkyminen kaikille ja kuulumisten sekä uutisten kertominen niille, joita se kiinnostaa.¨

Julkisen käyttötarkoituksensa vuoksi on kuitenkin vielä tärkeämpää pitää huolta siitä, ettei kerro yksityisiä asioitaan kaikille, vaikka niitä suurella todennäköisyydellä ei luekaan kuin kaveripiiri. Jokainen saa itse valita mieleisensä käyttäjätunnuksen, joten koskaan ei voi varmuudella tietää, kuka käyttäjää seuraa. Jos päätät haukkua kavereiden kesken pomoa, on riskinä, että yksi seuraajista onkin itse pomo.

5.2.1 Käyttäjätili

Jokaisella käyttäjällä on oma käyttäjätunnus, jonka saa itse valita, kunhan se on vapaa. Kissanhäntä eli @-merkki laitetaan aina käyttäjätunnuksen eteen, myös toisiin käyttäjiin viitatessa. (Heikniemi 2011, 47.)

Twitter on ilmainen ja siihen voi liittyä kuka tahansa ja kuka tahansa voi twiitata. Laittamansa twiitit näkevät he, jotka seuraavat käyttäjää ja samalla tavalla voi itse seurata haluamiansa henkilöitä ja nähdä heidän twiittinsä. Osa tileistä on myös yksityisiä, mutta ne ovat harvassa. Näitä käyttäjätilejä ei voi seurata ilman heidän hyväksyntäänsä. (Heikniemi 2011, 47.)

Kuva 12. Tilin asettaminen yksityiseksi.

Palvelu on siis hyvin samankaltainen kuin Facebookin tilaviestit, jotka näkyvät etusivulla. Ero on kuitenkin siinä, että Facebookissa kaikki ovat yksityishenkilöitä, joiden kaikki tiedot eivät näy ilman hyväksyttyä ystävyyssuhdetta. Twitterissä suhteet ovat enemmän yksipuolisia eli käyttäjä seuraa itseään kiinnostavia henkilöitä ja lisäksi Twitter on pääosin julkinen. Twitterin päätarkoituksena on päästä seuraamaan uusia keskustelunaiheita ja pysyä ajan tasalla kenties omien kiinnostuksen kohteiden kanssa esimerkiksi seuraamalla peliaiheisia uutissivustoja. (Heikniemi 2011, 47.)

Twitterin käyttöliittymä on hyvin pelkistetty, joten sitä voi käyttää kännykän kautta, mutta myös suoraan selaimella. Suurin osa aktiivikäyttäjistä käyttää Twitteriä erillisellä asiakasohjelmalla. Ne ovat pääsääntöisesti ilmaisia ja niitä on useita riippuen käytettävistä laitteista ja käyttöjärjestelmistä. Keskeiset ominaisuudet ovat kuitenkin samat: ohjelmilla voi seurata omaa syötettä sekä useita hakuja kerrallaan. Vastaamiseen ja muuhun on helpot toiminnot. Myös nykyisiin älypuhelimiin on tarjolla jonkin verran eri asiakasohjelmia, joilla tavallinen nettipohjainen käyttö onnistuu vaivattomasti. (Heikniemi 2011, 48.)

5.2.2 Uutiset, sää ja muut

Twitter on erinomainen väline, kun haluaa seurata tapahtumia reaaliajassa; sen kautta uutiset leviävät hyvin nopeasti. Kun on kohdistanut kiinnostuksensa uutistoimistoihin ja sopiviin henkilöihin kuten suosittuihin artisteihin, voi saada syötteeseensä ajantasaista tietoa uusista tapahtumista. Kun kerrot esimerkiksi paikkakunnallasi tapahtuvasta suurkolarista, käyttäjää seuraavat paikkakuntalaiset voivat helposti painaa retweet-nappia, joka lähettää saman viestin heidän seuraajilleen ja tällä tavalla uutinen leviää äärimmäisen nopeasti jo muutamalla painalluksella kenties tuhansille. Myös media onkii juttuvihjeitä Twitteristä. Nykyään esimerkiksi viihdeuutisissa on tavanomaista, että kerrotaan artistin twiittaamasta kuvasta tai muusta uutisesta. Pitää kuitenkin myös muistaa, että myös huhut liikkuvat, joten kaikkea lukemaansa ei kannata uskoa. (Heikniemi 2011, 47.)

Uutiset liikkuvat Twitterissä nopeasti, usein jopa virallisia uutissivuja nopeammin, koska tieto pääsee Twitterissä liikkumaan välittömästi. Esimerkiksi, kun Japania kohtasi yksi traagisimpia luonnonkatastrofeja maan historiassa maaliskuussa 2011, tieto liikkui Twitterissä hyvin nopeasti ja esimerkiksi sanalla tsunami saattoi seurata jatkuvasti ihmisten twiittauksia aiheeseen liittyen.

Samalla tavoin Twitteristä voi myös hakea nopeasti pika-arvosteluja muun muassa uusista levyistä. Arvostelut eivät ole pitkiä merkkimäärän rajoituksesta johtuen, mutta siitä selviää silti nopeasti, onko peruskäyttäjän mielestä uusi albumi huono vai hyvä, joskin ilman syvällisempää analyysiä. Twitterin haku on tosiaikainen eli se päivittyy koko ajan uusilla uutisilla. (Heikniemi 2011, 49.)

Twitter tarjoaa lisäksi mahdollisuuden kertoa sijaintinsa twiitissään (kuva 13). Jos kertoo profiilissaan ilotulituksesta, voi paikan kertomalla osoittaa kaikille, missä ilotulitus on meneillään. Paikan voi kertoa vaikka kaupungin mukaan, mutta myös tarkan sijainnin kertominen on mahdollista. Jos haluaa myöhemmin poistaa paikkahistoriaansa, se on mahdollista tehdä jälkeenpäin.

Kuva 13. Sijainnit.

5.2.3 Keskusteleminen

Twiitit voivat olla myös henkilökohtaisia, koska niitä lukevat monesti pelkästään kaveripiiriin kuuluvat henkilöt, vaikka ne olisivatkin julkisia ja niihin voidaan myös vastata. Tämä toimii yleensä kirjoittamalla julkinen viesti, jossa viitataan käyttäjän tunnukseen. Vastaus näkyy kaikille vastaajan seuraajille, sekä totta kai alkuperäisen kirjoittajan syötteessä, koska siinä mainitaan hänen nimensä. Myös yksityisesti on mahdollista kirjoitella henkilöille, jotka seuraavat käyttäjää. (Heikniemi 2011, 48.) Tämä onnistuu Direct Messagen avulla.

Itselleen sopivia keskustelunaiheita löytää hakemalla tai seuraamalla sopivien henkilöiden tekemisiä. Twitterissä on käytäntönä, että tiettyä asiaa koskevat viestit merkataan risuaidalla (#) ja asian nimellä. Näiden tunnisteiden avulla voidaan seurata eri aiheita riippumatta siitä, kuka niistä keskustelee. Voit kertoa esimerkiksi kokemuksestasi lempipelisi parissa ”Mahtava pelikokemus! #Finalfantasy”. Twitter ei tulkitse risumerkintöjä mitenkään, mutta muilla käyttäjillä saattaa olla seurannassa Twitter-haku sanalla #Finalfantasy, jolloin viestisi päätyvät heidän näkyvilleen haun kautta ja kenties he saattavat jopa alkaa seurata käyttäjää. (Heikniemi 2011, 48.)

Nämä erilaiset aihemerkinnät muodostavat kanavia, joita seuraamalla näet yhden aiheen keskustelun. Ne elävät koko ajan ja niitä voi luoda vapaasti nimeämällä uusia käsitteitä. Suosituimmat tapahtumat näkyvät myös Twitterin etusivulla olevien nostojen kautta: trending topics –otsikko kertoo, mitkä aiheet ovat sillä hetkellä suosituimmat. Puhutuimpia aiheita voi selata myös alueittain, tosin Suomeen hakua ei voi tällä hetkellä rajata. (Heikniemi 2011, 48.)

Kuvassa 14 näkyy esimerkkejä millaisia eri komentoja Twitterissä on mahdollista käyttää, jotta saa sovelluksesta kaiken mahdollisen irti.

Kuva 14. Komentoja.

5.2.4 Linkit, kuvat ja videot

Twitterissä liikkuu muutakin tietoa kuin teksti, koska aina merkkien määrä ei ole riittävä kertomaan haluttua asiaa. Siitä syystä Twitterissä liikkuu myös kuvia, videoita sekä runsaasti linkkejä. Myös paikkatiedot kulkevat Twitter-viesteissä. Halutessaan voi siis ilmoittaa, missä on viestinlähetyshetkellä esimerkiksi Twitter Mapsin avulla. (Heikniemi 2011, 49.)

140 merkkiä rajoittaa usein linkkien näkymisen oikeassa pituudessaan, joten Twitterissä käytetään paljon lyhennettyjä url-osoitteita. Esimerkiksi bit.ly-palvelu on yksi vaihtoehto osoitteiden lyhentämiseen. Minkä tahansa osoitteen voi lyhentää ja useimmat Twitterin asiakasohjelmista tekevät sen automaattisesti. (Heikniemi 2011, 49.)

Twitpic ja Twitvid ovat suosittuja palveluita kuvien ja videoiden linkittämiseen. Lisäksi ne tarjoavat myös lyhyitä osoitteita. Kun kuvan laittaa asiakasohjelmaan, se liittää kuvan automaattisesti Twitpiciin. Kuvat näkyvät twiitissä painettavina linkkeinä, vaikka niiden painaminen yleensä avaa kuvan suoraan asiakasohjelmaan. Lisäksi kuvat näkyvät Twitpicin sivustolla ja sinne kirjoitetut kommentit näkyvät Twitterin kautta kuvan lähettäjälle. (Heikniemi 2011, 49.)

Twitterissä liikkuu myös paljon huijareita eli henkilöitä, jotka saattavat esiintyä esimerkiksi tunnettuina julkisuuden henkilöinä, jotka eivät itse Twitteriä käytä ja tällä tavalla he keräävät itselleen mahdollisesti valtaviakin määriä seuraajia. Sitten huijarit voivat laittaa harmillisia linkkejä esille julkaisuissaan, jolloin seuraajat painavat niitä ja tällä tavalla haittaohjelmatkin pääsevät leviämään.

5.2.5 Yritystoiminta

Monet yritykset ovat siirtäneet asiakaspalvelunsakin Twitteriin varsinkin USA:ssa. Yrityksiä löytyy muun muassa lentoyhtiöistä ja hotelleista, jotka tarjoavat ongelmanselvitystä Twitterissä. Monesti ei tarvitse edes itse hakea apua, sillä monet ohjelmien tekijät ja yritykset seuraavat jatkuvasti omiin tuotteisiinsa liittyvää Twitter-liikennettä ja jopa vastaavat viesteihin. Joten jos

valittaa saamastaan huonosta kohtelusta, voi saada yrityksen taholta pahoittelun ja joskus jopa korvauksia. (Heikniemi 2011, 49.)

5.2.6 Palvelurobotit

Twitter on täynnä palvelurobotteja, tuttavallisemmin botteja. Twitterin kanssa on toteutettu useita erilaisia palveluita, jotka voivat pohjautua erilaisten nopeiden tiedonantojen jakeluun tai käyttäjien väliseen viestintään. Käyttäjä voi esimerkiksi seurata missä hänen tilaamansa paketti kulloinkin liikkuu tai saada itselleen muistutuksen tv-ohjelmasta. Kaikki on kiinni siitä, mitä toimintoa haluaa ja alkaa sitten seurata ja käyttää palvelua. Vaihtoehtoja on runsaasti ja ne ovat paras tapa perehtyä kaikkeen, mitä Twitterissä tapahtuu ja mitä sillä on tarjota. Myös henkilöhaun avulla voi etsiä ihmisiä kiinnostuksen kohteiden mukaan ja löytää uusia tuttavuuksia. (Heikniemi 2011, 49.)

Twitter on lisäksi täynnä palvelurobotteja, jotka automaattisesti alkavat seurata käyttäjiä. Jos käyttäjä alkaa esimerkiksi seurata jotain suosikkiartistiaan, voi olla, että artistin listalla oleva botti alkaa automaattisesti seurata myös häntä. Nämä palvelurobotit eivät ole oikeita ihmisiä, vaan sen sijaan palveluntarjoajia, jotka tällä tavalla hakevat huomiota. Huomatessaan seuraajan käyttäjä voi katsoa mistä on kyse ja huomatessaan sen liittyvän omaan kiinnostuksen kohteeseensa, käyttäjä voi alkaa seurata palvelua.

Automaattisesti seuraavat botit voivat kuitenkin aiheuttaa ongelmia, vaikka sivu näyttäisi harmittomalta ja vaikka joku tuttukin seuraisi tätä. Käyttäjä voi luulla botin liittyvän omaan kiinnostuksen kohteeseensa ja alkaessaan seurata tätä, voi jaettujen linkkienkin painaminen tuntua hyvältä ja mielenkiintoiselta idealta, mutta oikeasti kyseessä voi olla jälleen kerran haittaohjelmien leviäminen.

5.2.7 HTTPS

Myös Twitter tarjoaa nykyään mahdollisuuden käyttää palveluaan koko ajan salatulla yhteydellä. Aivan kuten aiemmin on mainittu, yhteys on tarpeellinen varsinkin silloin, kun sovellusta käyttää julkisissa koneissa tai muuten koneissa,

joiden turvallisuusasetuksista ei ole tietoa. Menemällä tilin asetuksiin, on mahdollista muuttaa suojaustaan (kuva 15).

Kuva 15. HTTPS-asetukset.

5.3 MySpacen tietoturva ja -suoja

Vaikka MySpacen suosio onkin vuosien saatossa laskenut, sillä on silti edelleen paljon aktiivisia käyttäjiä. MySpace sisältää paljon erilaisia ominaisuuksia, joista voi säätää profiiliaan oman näköisekseen. Sivustolla on mahdollisuuksia käyttää sitä useaan eri käyttötarkoitukseen riippuen omasta mielenkiinnosta ja kenties jopa alastaan. MySpacea voi käyttää joko yksityisenä tai julkisena henkilönä ja asetuksia onkin syytä säätää sen mukaan.

MySpace tarjoaa laajoja mahdollisuuksia esimerkiksi seuranhakuun, musiikin levittämiseen artistina tai ihan vain ystävien keskeiseen yhteydenpitoon. Sivustolla on mahdollista pitää blogia, pelata pelejä, jakaa valokuvia ja olla tekemisissä muiden käyttäjien kanssa juuri sen verran kuin itse haluaa ja kokee tarpeelliseksi.

Aivan kuten muissakin sosiaalisissa medioissa, ohjeita sivuston käyttämiseen löytyy helposti ja laajasti. Niihin onkin syytä tutustua tarkkaan ainakin silloin, jos ei ole vielä varma, kuinka julkisen profiilin haluaa tai mihin MySpacea haluaa käyttää. MySpace tarjoaa myös turvallisuusvinkkejä.

5.3.1 Profiili

MySpacen asetuksista saadaan säädettyä muun muassa profiilia koskevia ominaisuuksia halutunlaisiksi. Yleensä on kannattavinta muuttaa suositusasetukset tiukemmiksi jo heti alussa, jotta kaikki tiedot eivät olisi myös kolmansien osapuolien, kuten mainostajien, käytettävissä. Profiilin tarkasteluun voidaan esimerkiksi antaa lupa joko kaikille, vain ystäville tai vain ystäville ja

kaikille yli 18-vuotiaille. Tietoturvallisuuden kannalta järkevin vaihtoehto on vain ystäville, jos on kyseessä yksityishenkilö.

Profiilia säädettäessä voi laittaa syntymäpäivätietonsa näkymään ystäville. Uusia ystäviä on mahdollista etsiä iän mukaan joko sallimalla tai estämällä alle 18-vuotiaiden yhteydenotot. Jos käyttäjä merkitsee iäkseen 13-15 vuotta, nämä profiilit ovat automaattisesti yksityisiä.

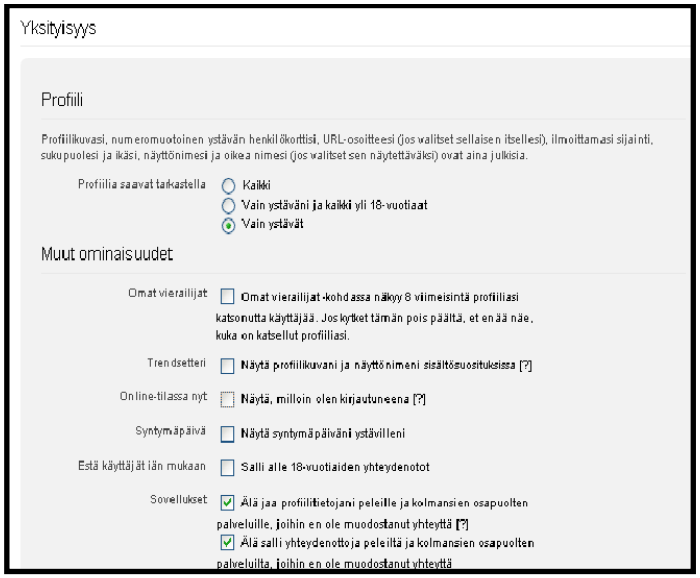
Profiilissa näkyvät viimeisimmät päivitykset, oli kyse sitten blogista, ystävistä, kommenteista, aktiviteeteista tai kunniamerkeistä. Kunniamerkkejä kerätään esimerkiksi siitä, kuinka monta kertaa muiden profiileissa on vieraillut tai kuinka usein profiiliaan on muokannut. Toisin sanoen MySpace ikään kuin palkitsee käyttäjää aktiivisuudestaan. Tämä on myös helppo keino osoittaa esimerkiksi ystäville, kuinka aktiivinen käyttäjä on sivustolla.

Nykyisin MySpacessa on otettu käyttöön uusi profiili, josta voi säädellä profiiliaan vieläkin helpommin ja sen saa näkymään jopa valokuvissa ja videoissaan. MySpace on täynnä moduuleja kuten aktiviteetit, blogit ja kommentit. Käyttäjä voi itse päättää, mitkä niistä hän haluaa profiilissaan näyttää. Niitä voi lisätä sivuille oman mielen mukaan ja muokata mieleisekseen. Tällä tavalla jokaisen käyttäjän profiilista on mahdollista tehdä oman näköinen ja uniikki.

Omista jutuista näkee kaikki MySpacen eri osat ja lisäksi sieltä pääsee käyttäjätilinasetuksiin, muokkaamaan profiilia, yksityisyydensuojan asetuksiin sekä ohjeisiin. Ohjeista löytyy MySpacen turvallisuusosio, johon kannattaa tutustua. Osiossa on kiinnitetty huomiota erityisesti teini-ikäisten turvalliseen nettikäyttäytymiseen. Siellä on myös tieto siitä, keneen ottaa yhteyttä, jos tuntee olonsa turvattomaksi verkossa.

Kun tuntematon käyttäjä ottaa yhteyttä, varsinkin jos kyseessä on vanhempi henkilö, joka ottaa yhteyttä huomattavasti nuorempaan henkilöön, voidaan hänen myöhempi yhteydenottonsa estää. Jos tuntematon yhteydenottaja tuntuu uhkaavalta ja epämieluisalta millään tavalla, hänestä voidaan ilmoittaa vanhemmille tai viranomaisille sekä raportoida MySpacelle. Turvallisuutta

voidaan parantaa myös esihyväksymällä kaikki profiiliin kirjoitetut kommentit ja ottamalla ”online-tilassa nyt” – tilakuvake pois päältä. Kuvassa 16 näkyy profiilin yksityisyysasetukset.



Kuva 16. MySpacen yksityisyysasetukset.

Jos on kiinnostunut saamaan laajasti kävijöitä sivulleen esimerkiksi aloittelevana artistina, käyttäjän on mahdollista jakaa profiiliaan Twitteriin, Facebookiin sekä Yahoohon tai vaikka näihin kaikkiin. Tietoturvaa ajatellen tämä ei välttämättä ole kannattavaa, sillä käyttäjä saattaa olla MySpacessa aloittelevana artistina, mutta muualla yksityisenä henkilönä. Kannattaa miettiä tarkkaan, haluaako pitää nämä osiot erillään vai yhdistää ne, jolloin kaikki sanomiset yhdessä mediassa yhdistetään mielipiteenä kaikkiin muihinkin.

5.3.2 Muut ominaisuudet

Yksityisyysasetusten kautta Omat vierailijat -kohdasta käyttäjä voi valita, haluaako nähdä, keitä hänen sivullaan vierailee. Tällöin käyttäjä näkee kahdeksan viimeisintä vierailijaa. (MySpace 2011a.)

Halutessaan voi asettaa Trendsetterin näyttämään käyttäjän profiilikuvan ja näyttönimen sisältösuosituksissa. Toisin sanoen esimerkiksi artistin sivulla vieraillessa näkyy profiili myös muille samalla sivustolla vieraileville henkilöille,

jotka voivat kiinnostuessaan käydä katsomassa käyttäjän profiilia. Jos ei ole kiinnostunut suuresta määrästä tuntemattomia käyttäjiä vierailemassa sivullaan, asetusta ei kannata ottaa käyttöön.

Muille käyttäjille on myös mahdollista näyttää, koska on kirjautuneena Online tilassa nyt – valikon kautta. Tämänkin voi halutessaan ottaa pois päältä, jolloin muut henkilöt eivät tiedä, koska käyttäjä on paikalla ja kuinka usein. Jotkut haluavat pitää tarkemmin kiinni yksityisyydestään, joten jos ei halua kaikkien tietävän aktiivisuudestaan, tämänkin voi muuttaa mieleisekseen.

Sovellusten kautta voi säätää, haluaako profiilitietojaan jakaa peleille ja kolmansien osapuolten palveluille, joihin yhteyttä ei ole muodostettu. Käyttäjä voi myös sallia tai olla sallimatta yhteydenotot peleiltä sekä kolmansien osapuolten palveluilta, joihin yhteyttä ei ole muodostettu. Jos ei halua ylimääräisiä sähköposteja MySpacen yhteistyökumppaneilta tai edes ohjelmilta, joita käyttää, on parasta olla sallimatta toiminto. Vaikka MySpace onkin voinut todeta yhteistyökumppaninsa luotettaviksi, se ei tarkoita, että itse olisi kiinnostunut saamaan heiltä kuitenkaan tiedotteita.

MySpacessa on kohokohdat - toiminto, joka ei näytä viimeisimpiä tiloja, vaan sen kautta aukeaa valikko kaikille aiheille. Näistä aiheista valitsemalla näkee vain kyseiseen aiheeseen liittyvät merkinnät. Julkaisuissa kannattaa jälleen kerran miettiä julkaisun aiheen sopivuutta sekä sitä, keille kaikille julkaisujaan haluaa näyttää. Laajimmilleen julkaisunsa voi näyttää kaikille ystäville, mutta jälleen on hyvä miettiä haluaako sitä valita, varsinkaan, jos profiilissa on paljon tuntemattomia ”ystäviä”.

Lisäksi MySpacesta löytyy myös Facebookin seinää vastaava Koti-toiminto. Kotona voidaan jakaa kuvia, linkkejä, videoita, musiikkia sekä kertoa käyttäjän tilasta ja mielialasta. Kannattaa kuitenkin harkita ennen kuin julkaisee mielialaansa, ettei se ole ristiriidassa oikean olotilan kanssa. Esimerkiksi sairaslomalla olevan ei kannata kertoa voivansa erinomaisesti. Aivan mitä tahansa ei myöskään kannata kirjoittaa itseään kiinnostaviin juttuihin. Julkinen

profiili näkyy kaikille ja jos kirjoitat esimerkiksi huumorimielessä harrastavasi mummojen potkimista, se ei anna hyvää kuvaa.

5.3.3 Seuranhaku

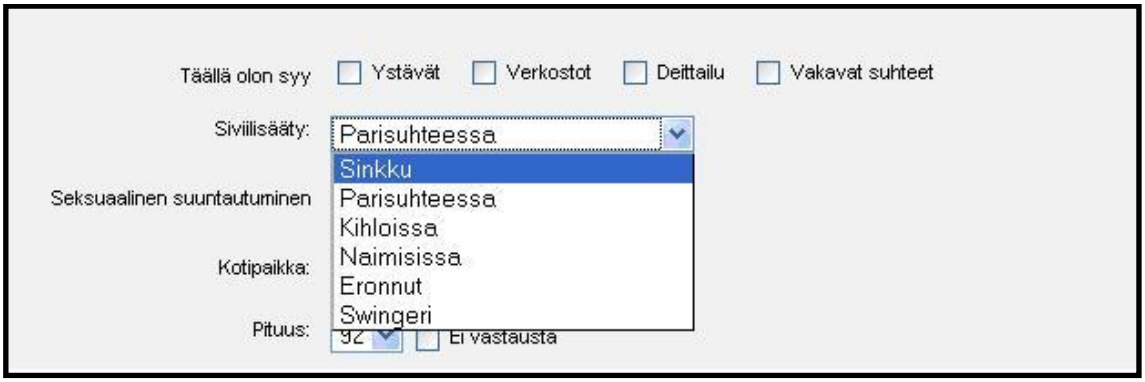
MySpacen kautta myös seuranhaku on mahdollista ja asetusten kautta on mahdollista säätää profiilitietojaan hyvinkin tarkasti. Käyttäjä voi määritellä muun muassa MySpaceen liittymisen syyt, suhteensa esimerkiksi lapsiin ja alkoholiin ja myös tulonsa on mahdollista tuoda julki. Vaihtoehtoja jokaiseen kohtaan on useita ja niistä löytää suurella todennäköisyydellä itselleen sopivan vaihtoehdon.

Tietoturvan kannalta ei ehkä ole järkevää ilmoittaa tulojaan julkisesti, vaikka niitä ei tarkasti voikaan määritellä. Seuraa hakiessa tulojenkin kertominen voi osoittaa tietynlaisesta statuksesta, jonka haluaa tuoda julki. Se, onko tulojen kertominen tarpeellista, on taas toinen täysin eri asia. MySpacessakin saattaa kuitenkin liikkua myös huijareita, jotka kertovat tulonsa yläkanttiin. Samalla tavalla kaikista muistakin kiinnostuksen kohteistaan voi valehdella vain, jotta saisi mieleistä seuraa.

Kuvasta 17 näkee, millaisia erilaisia vaihtoehtoja käyttäjän on mahdollista määritellä profiilissaan ja seuranhaussaan. Lisäksi kuvasta näkyy ominaisuuksia, joiden perusteella seuralaisen hakua voidaan rajoittaa. Kriteereinä voi olla esimerkiksi valokuvan olemassaolo, ikä, sukupuoli tai asuinpaikka.

Kuva 17. Seuranhaku.

Kehittyneemmässä haussa on mahdollista rajoittaa hakuaan vieläkin yksityiskohtaisemmin. Tällaisia kriteereitä voivat olla muun muassa siviilisääty, seksuaalinen suuntautuminen tai vaikka vartalotyyppi. Kuva 18 näyttää esimerkin siviilisäädyn eri vaihtoehdoista. (MySpace 2011b.)



Kuva 18. Siviilisääty hakukriteerinä.

5.3.4 Pikaviestit

Pikaviesteissä on sekä hyviä että huonoja ominaisuuksia. Pikaviestit ovat helppo, nopea ja ilmainen tapa, eikä se ole ajasta riippuvainen. Useiden henkilöiden kanssa pikaviestittäminen voi kuitenkin johtaa yllättäviin vahinkoihin ja ongelmiin, kun käyttäjän lähettämä mustamaalausviesti ei menekään kaverille, vaan mustamaalauksen kohteelle. Viestit voivat helposti mennä vääriin paikkoihin. Koskaan ei tiedä kuinka monta henkilöä on itse asiassa lukemassa viestejäsi.

Pikaviestien luonne on nopeatempoinen tiedonvaihto, jossa sattuu paljon kirjoitusvirheitä ja helppoja väärinymmärryksiä. Viestien tiedonkulku on usein oheistoimintaa, jota ihmiset tekevät samaan aikaan kun pelaavat tai toisten juttuja lukiessa. Toista kirjoittajaa ei näe kirjoitus- ja lukuhetkellä, joten sarkastiseksi tarkoitettu viesti saattaa lukijan mielessä kääntyä vihaiseksi, lukija ei siis tiedä varmasti, millä mielellä toinen osallistuu viestien kirjoittamiseen. Tästä syystä väärinkäsityksiä voi syntyä helposti. Kuvassa 19 näytetään miten pikaviestintää voidaan käyttää.

Kuva 19. Esittelee pikaviestien toimintaa (MySpace 2011c).

5.3.5 Rikollisuus MySpacessa

MySpacesta ei ole paljon uutisointia mediassa, koska käyttäjien määrä laskee jatkuvasti. Hakkerit ja muut rikolliset eivät enää ole yhtä kiinnostuneita sivustosta kuten ennen.

Vuonna 2007 MySpace joutui poistamaan sivuiltaan noin 30 000 profiilia, koska kyseisillä henkilöillä oli tuomio seksuaalirikoksesta. Yhdysvalloissa useat teini-ikäiset olivat joutuneet pedofiilien hyväksikäyttämiksi tapaamisissa tutustuessaan heihin ensin MySpacen kautta. (Reuters 2007.)

5.3.6 MySpacen vinkit teini-ikäisille

Ikäänsä ei pidä valehdella, sillä MySpacen alaikäraja on 13 vuotta. MySpace poistaa käyttöoikeudet kaikilta, jotka valehtelevat ikänsä tai ovat alle 13-vuotiaita.

MySpace on julkinen sivusto ja tästä syystä jäsenten ei tulisi kertoa tai julkaista itsestään mitään, mitä ei olisi valmis kertomaan koko maailmalle. Erityisen tarkkana pitää olla valokuvien suhteen, jos ei halua kolmansien osapuolten saavan tietoonsa esimerkiksi opiskelupaikkakuntaa. Mitään noloa ei myöskään tulisi koskaan julkaista itsestään tai muista.

Hyväksy kavereiksi vain tuttuja henkilöitä. Tuntemattomien tapaamista pitää välttää, koska ihmiset eivät ole aina niitä, joita he väittävät olevansa. Varsinkin nuorten on hyvä pitää mielessä, että uusia ihmisiä tavatessa asiasta pitäisi aina kertoa vanhemmille, eikä tapaamisiin saisi mennä yksin.

Ahdistelusta, mustamaalaamisesta ja sopimattomasta sisällöstä tulisi tehdä ilmoitus, vaikka niistä aiheutunut harmi ei olisikaan aiheuttanut suuria ongelmia. Tällä tavalla voidaan estää ongelmien kasvaminen ja kitkeä ne pois heti alkuunsa.

Kaikkia julkaisujaan pitää aina miettiä tarkkaan ennen niiden tekemistä. Kaikki julkaistu materiaali on kenen tahansa ladattavissa ja ne voivat säilyä Internetissä ikuisesti. Myös nettikiusaaminen on nykyään normaalia ja

julkaistulla materiaalilla voidaan myös kiristää käyttäjää. Kuva 20 näyttää, kuinka MySpace painottaa tietoturvaa teini-ikäisille sekä heidän vanhemmilleen.

Kuva 20. Ohjeita MySpacen turvalliseen käyttöön.

6 Yleisohjeet

Sosiaalisessa mediassa, kuten Internetissä muutenkin, hölmöily saattaa pahimmassa tapauksessa viedä työn, tyhjentää pankkitilin tai lopettaa ihmissuhteita.

Vaikka periaatteessa käyttäjät ovat sosiaalisessa mediassa yksityishenkilöitä, se ei tarkoita, että voi käyttäytyä miten tahansa. Yksi tärkeä ohje esimerkiksi on, ettei koskaan saisi haukkua, mustamaalata, kiusata tai kirjoittaa pahoja asioita toisista henkilöistä, esimerkiksi työnantajastaan. Varsinkin silloin, kun käyttäjä kertoo profiilissaan työnantajansa, hän on tällöin samalla ikään kuin yrityksen edustajana. (VAHTI 2010, 36.) Jos alkaa mustamaalata työnantajaansa, on hyvin suuri todennäköisyys, että tieto jotenkin päätyy jossain vaiheessa myös esimiehen korviin, jolloin voi saada potkut. Myös maineen menetyksen riski on suuri, sillä tällaiset jutut liikkuvat. Jos asiasta tulee missään määrin julkinen tai jos työnantajat puhuvat keskenään, voi olla vaikea saada uusia töitä varsinkaan omalta alaltaan.

Huomionarvoista on myös, että työntekijän omat henkilökohtaiset mielipiteet saatetaan nähdä organisaation mielipiteinä. Jos työntekijä tuo esille esimerkiksi homovastaisuutensa, voivat muut nähdä tämän yrityksen yleisenä mielipiteenä ja alkaa boikotoida esimerkiksi yrityksen tuotteita ja julistaa muita tekemään

samoin. Imagon korjaaminen voi olla jopa mahdotonta ja kun maine on menetetty, koko yritys saattaa olla menetetty. Myös väärennetyt ja kaapatut profiilit saattavat tahallaan alkaa mustamaalata yritystä. (VAHTI 2010, 22.)

Suomessakin on päädytty jo useisiin irtisanomisiin, jotka johtuvat työntekijän kirjoittamasta kritiikistä työpaikastaan. Tapaukset tulevat suurella todennäköisyydellä yleistymään lähivuosina. Tapauksesta riippuen yritys on voinut menetellä oikein, mutta neuvotteluihin lähdetään myös ja tarvittaessa oikeuteenkin, jos on tarvetta. Osa yrityksistä on maksanut irtisanomisesta korvauksia ja osa on ottanut työntekijän myös takaisin töihin. Joskus myös pelkkä anteeksipyyntö työntekijän osalta riittää sovun saavuttamiseksi. (Niiles 2011.)

Työasioista ei kannata keskustella muualla kuin työtehtäviin hyväksytyissä sosiaalisissa medioissa. On pidettävä tarkkaan huoli siitä, ettei vuoda salaisia yritystietoja muualle kuin sille tarkoitetulle alustalle, jotta organisaation tietovuodot voidaan välttää. Lisäksi on muistettava, että palvelun ylläpitäjät pääsevät teknisesti käsiksi kaikkeen tietoon, joka sosiaalisessa mediassa liikkuu. Tällaista tietoa voivat olla esimerkiksi kahden henkilön väliset yksityiskeskustelut. (VAHTI 2010, 36.)

Samalla tavalla vähänkin julkisemman profiilin kanssa kannattaa miettiä muutenkin tarkemmin, mitä julkaisee. Esimerkiksi kavereille näytettävä video voi olla hauska, mutta onko se sopivaa ammattia ajatellen. Lisäksi se myös näkyy kaikille. Onkin tarkkaan mietittävä, kannattaako kaverikseen ottaa esimerkiksi työnantajaansa tai oppilaitaan. Ohjeistuksena voisi antaa, ettei se ole kannattavaa. On luonnollista haluta pitää erikseen työminä ja arkiminä ja se pätee myös sosiaalisessa mediassa.

Rikolliset, ääriryhmät sekä valtio pyrkivät verkossa saamaan haltuunsa muun muassa henkilötietoja ja yrityssalaisuuksia. Ne haluavat vaikuttaa käyttäjien päätöksentekoon ja lisäksi ne voivat myös koettaa tahrata käyttäjien sekä organisaatioiden maineen (Pitkänen 2010 c).

Jos ei ole täysin varma sosiaalisessa mediassa liikkuvan linkin turvallisuudesta ja alkuperästä, sitä ei kannata painaa. Tällä tavalla liikkuu paljon haittaohjelmia, jolloin käyttäjän kone voidaan saada haltuun. Väärinkäyttäjillä saattaa olla tuhansista kaapatuista koneista koostuva ns. botnet-verkko, joka toimii esimerkiksi tehokkaana roskapostipalvelinympäristönä tai se voi laskennallisesti kokeilla erilaisia salasanoja päästäkseen koneeseen käsiksi. (VAHTI 2010, 13.) Käyttötapoja on useita, mutta lopputulokset eivät varmasti ole käyttäjän kannalta mieluisia.

Jos käyttäjästä tuntuu, että hän on joutunut huijauksen kohteeksi, on tärkeää ottaa välittömästi yhteyttä viranomaisiin, ennen kuin ongelma ehtii kasvaa liian isoksi. Rikosilmoitus kannattaa tehdä aina, vaikka suurta taloudellista menetystä ei olisikaan tapahtunut. (VAHTI 2010, 36.)

Salasana on yksi oleellisimmasta asioista tietoturvaan liittyen. On ehdottoman tärkeää, ettei samaa salasanaa käytetä useassa eri paikassa varsinkaan saman käyttäjätunnuksen kanssa. Jos käyttää sosiaalisia medioita työn puolesta, on tärkeää, ettei työn puolella ole samaa salasanaa kuin yksityisellä puolella. (VAHTI 2010, 36.) Salasanan kuuluu olla vahva eli sen täytyy olla vähintään 8 merkkiä pitkä, sisältää pieniä ja suuria kirjaimia sekä numeroita ja erikoismerkkejä, eikä salasanan kuulu tarkoittaa mitään. Huonoa tietoturvaa osoittaa myös oikean sanan käyttö, mutta kirjainten muuttaminen samannäköiseksi numeroksi esimerkiksi ”numero” onkin ”num3r0”, sillä tällaisten salasanojen murtaminen ei ole aikaa vievää.

Liian henkilökohtaista tietoa ei pidä laittaa esille. Tämä tarkoittaa sähköpostiosoitetta, oikeaa osoitetta, puhelinnumeroa ja muita vastaavanlaisia tietoja. Lisäksi ohjeeseen kuuluvat valokuvat ja muu materiaali itsestään. Täytyy ottaa huomioon, että monilla palveluntarjoajilla on oikeus syötettyjen tietojen käyttämiseen hyvinkin laajasti, sekä oikeus antaa tietoja eteenpäin yhteistyökumppaneille. On tärkeää tutustua sopimusehtoihin ennen sosiaalisten palveluiden käyttöönottoa. (VAHTI 2010, 36.)

Käyttäjäprofiilin yksityisyyden suojaa koskevat asetukset pitäisi aina muistaa tarkistaa ennen tietojen lisäämistä. Palvelun muodosta riippuen ne pitää muuttaa joko yksityisiksi tai julkisiksi ja tarkistaa, mitkä tiedot ovat näkyvillä. Vaikka profiili olisi julkinen, esimerkiksi sähköpostiosoitteen kertominen ei välttämättä ole suositeltua. Jos profiili on yksityinen, pitää tarkistaa, että tiedot näkyvät vain niille henkilöille, joille haluaa niiden näkyvän. Tällöinkään ei kannata välttämättä laittaa kaikkia tietojaan esille, kuten osoitetta tai puhelinnumeroa. Tällä tavalla estetään tietojen leviäminen laajemmalle kuin on tarkoitettu. (VAHTI 2010, 36.)

Perheen ja ystävien yksityisyyttä täytyy kunnioittaa. Vaikka itse käyttäisi aktiivisesti sosiaalisia medioita ja jakaisi aktiivisesti valokuvia kaikille tutuille, muut eivät välttämättä ole asiasta yhtä innostuneita. Jos he eivät halua itsestään kuvia julkisesti esille, halua pitää kunnioittaa, eikä mitään saa julkaista ennen kuin on kysytty etukäteen suostumusta. (VAHTI 2010, 36.) Jos kuvan poistaa jälkeenpäin erillisestä pyynnöstä, voi olla jo liian myöhäistä. Mitään muitakaan tietoja ei saa julkaista ilman heidän lupaansa.

Verkostoon ei saisi hyväksyä tuntemattomia yhteydenottoja (VAHTI 2010, 36). Jos ei itse henkilökohtaisesti tunne yhteydenottajaa, on parasta hylätä pyyntö. Vaikka kyseessä olisikin kaverin kaveri, ei ole suositeltavaa hyväksyä pyyntöä. Ei ole mitään syytä ottaa tuntemattomia listaansa, sillä käyttäjä ei tiedä heistä tai heidän tarkoitusperistään yhtään mitään.

On myös hyvä muistaa pitää oma kone aina ajan tasalla. Käyttöjärjestelmäpäivitysten on oleellista olla päivitettyinä ja on pidettävä huoli tarvittavista palomuuri- ja haittaohjelmien torjuntaohjelmistojen käytöstä sekä niiden automaattisesta päivittämisestä. (VAHTI 2010, 37.) On oltava tarkkana, että käytetyt ohjelmat ovat varmasti virallisia.

Syntymäaikaa tai -paikkaa ei välttämättä ole suositeltua kertoa, sillä Yhdysvalloissa on tullut ilmi tapauksia, joissa sosiaaliturvanumeroita on pystytty jäljittämään syntymäajan perusteella. Mieluummin kannattaa laittaa lähellä omaa syntymäpäiväänsä oleva päiväys. (Smith & Bosker 2011.)

Sopimattomia kuvia sosiaalisissa medioissa ei koskaan saisi julkaista. Ne johtavat helposti vaikeuksiin. Vaikka tulisi jälkeenpäin katumapäälle ja päättää poistaa kuvan, se voi silti palata kummittelemaan. Palvelujen palvelimet voivat varastoida kuvia ennalta arvaamattoman ajan, joten jopa poistettuihin kuviin on mahdollista päästä käsiksi jälkeenpäin. (Smith & Bosker 2011.) Myös muut käyttäjät voivat ottaa kuvia talteen ja käyttää niitä julkaisijaa vastaan tai muuten levittää kuvia Internetissä.

Sopimattomiin kuviin voidaan luokitella myös kuvat asunnosta, jotka paljastavat sen pohjapiirroksen tai kodin arvotavarat (Smith & Bosker 2011). Tämä antaa murtovarkaille vielä enemmän syytä päästä murtautumaan kotiin ja viemään kaikkea arvokasta ja se herättää myös enemmän kiinnostusta alkaa seurata käyttäjän tekemisiä tarkemmin eli sitä, milloin tämä on poissa kotoa.

Tunnustuksia ei kannata julkaista esimerkiksi siitä, kuinka verotuksessa on huijattu tai kuinka hyvin kaupan ryöstäminen juuri onnistui. Tällaiset julistukset ovat todistusaineistoa, jota voi olla vaikea poistaa ja estää sen leviämistä. Monet vakuutusyhtiöt ja jopa poliisi seuraavat nykyään tarkkaan sosiaalisia medioita selvittääkseen rikoksia. (Smith & Bosker 2011.) Varsinkin nuoret saattavat kertoa helposti hauskanpidostaan näpistelyn parissa ymmärtämättä, että kaikki näkevät sen ja teolla voi olla seurauksia. Ei ole myöskään täysin tavatonta, että henkilö, joka haluaa olla ”kadonnut”, on paljastanut olinpaikkansa kirjoittamalla Facebookiin esimerkiksi kaverin profiilin kautta.

Sosiaalisissa medioissa ei myöskään kannata kertoa loma-aikeistaan, olivat ne sitten lyhyt- tai pitkäaikaisia. Lähtölaskennat matkalle lähtöön ovat huono idea, sillä ne antavat murtovarkaille enemmän aikaa suunnitella, mutta myös pelkkä tunnin varoaika voi riittää. Jo pelkkä päiväreissusta kertominen voi päättyä siihen, että kotiin palatessa on talo tyhjänä. Huomattavasti parempi tapa on kertoa jälkeenpäin olleensa matkoilla, tällä tavalla murtovarkaat eivät voi iskeä. (Smith & Bosker 2011.)

7 Pohdinta

Sosiaalisessa mediassa pätevät samat ohjeet kuin Internetissä yleensä eli ei kannata julkaista mitään, mitä ei ole valmis näyttämään kaikkialla ja kaikille. Minkä kerran laittaa Internetiin, se on siellä ikuisesti jossain muodossa, eikä sitä saa pois enää koskaan. Terveen järjen käyttö on sallittua ja suositeltavaa. Vaikka sosiaaliset mediat ovat erilaisia ja sisällöt niissä erilaisia, toimintatavoiltaan ne ovat loppujen lopuksi hyvin samankaltaisia.

Ihmisten suhtautuminen sosiaaliseen mediaan vaihtelee, mutta selvää on, että kiinnostus sitä kohtaan ja sen antamia mahdollisuuksia kohtaan kasvaa koko ajan. Rikolliset tahot, työnantajat, poliisi, armeija, vakuutusyhtiöt, mainostajat ja yksityiset ihmiset käyttävät sosiaalisia medioita omiin tarkoitusperiinsä ja vain aika näyttää kuka heistä hyötyy siitä eniten.

Kun miettii, kuinka paljon tietoa nykyaikana on käytössä varsinkin Internetin kautta ja kuinka helposti kaikki tieto on saatavilla, on omituista, kuinka paljon virheitä ihmiset tekevät. Vaikka yritykset, nettisivut sekä lukuisat muut tahot korostavat esimerkiksi sitä, etteivät kysy milloinkaan eivätkä missään tapauksessa salasanoja, silti ihmiset tuntuvat jakavan niitä eteenpäin, kun sähköpostiin tulee huonolla suomella kirjoitettu ilmoitus ”tietoturvavuodosta”. Kehitys on ollut niin nopeaa, etteivät ihmiset ole vielä sisäistäneet kaikkia mahdollisuuksia sekä totta kai niiden tuomia ongelmia.

Ehkä ongelmana voidaan kuitenkin nähdä myös tiedon helppo saanti sekä tiedon runsas määrä. Nykyaikanamme vallitsee tiedon liikatarjonta. Enää ei tarvitse ottaa selvää asioista erikseen, vaan kaikki tieto tarjotaan valmiina, kunnes käyttäjä itse sitä haluaa käytettävän. Tästä syystä johtuen ei ehkä jakseta tutustua rekisteröinnin yhteydessä vaikkapa sopimusehtoihin, luki siellä mitä tahansa. Ihmiset olettavat kaiken olevan kunnossa, eikä heidän tarvitse sitä erikseen lukea läpi.

Yksi hyvä esimerkki tästä on aprillipila, jonka pelikauppa GameStation teki vuonna 2010. He laittoivat sopimusehtoihin, että sopimukseen suostuvat antavat heille sielunsa. Yritys keräsikin päivän aikana aimo kasan sieluja, noin

7000 henkilöä hyväksyi sen. Sopimukset kuitenkin purettiin, kun aprillipäivä oli ohi. (Schram 2010.)

Varsinkin nuorten luulisi olevan perillä asioista, mutta luultavasti asia on niin, että he ovat täysin tietämättömiä tietoturvasta, riskeistä sekä seurauksista, joita sopimaton käyttäytyminen ja kuvat voivat aiheuttaa. Tämän voidaan ajatella johtuvan siitä, että he ovat ikään kuin aina kasvaneet tietokoneen parissa, kaikki on heille aina ollut jokapäiväistä ja siksi Internetissä liikkumiseen suhtaudutaan samanlaisella asenteella eli se on vain yksi jokapäiväinen normaali tehtävä.

Tästä syystä ei osata ajatella asiaa pidemmälle ennen kuin vanhempana, kun se yksi kuva tulee esille työhaastattelussa. Nuoret tekevät kaikkea typerää ja oppivat virheistään kantapään kautta. Ongelmana on, että ennen tekemiset eivät jääneet mihinkään pysyvään rekisteriin, vaan aikuiseksi kasvettaessa jäivät tehdyt typeryydetkin pelkkinä muistoina menneisyyteen. Nykyään se ei enää onnistu, kaikki jää talteen ja sen sijaan, että nuoret jättäisivät tekonsa menneisyyteen, ne saattavatkin tulla kummittelemaan loppuelämäksi.

Sosiaaliset mediat ovat riskialttiita siinä mielessä, että se kokoaa paljon ihmisiä samaan paikkaan ja kaikki ovat yhteydessä toisiinsa. Periaatteessa mediassa pitäisi olla koko ajan varuillaan ja miettiä tekemisiään sekä sanomisiaan, mutta asiaa ei nähdä näin. Se on vain yksi alusta muiden joukossa. Alusta, jossa jakaa kokemuksiaan ja kuviaan kaikille, kenties saadakseen huomiota. Varsinkin julkisuudenhakuisuus tuntuu olevan yleistä nyky-yhteiskunnassamme. Sosiaaliset mediat, kuten Internet yleensäkin, antavat tälle hyvän pohjan ja ne tuovat käyttäjän esille massasta, jos tämä vain haluaa ja tekee kaikkensa asian eteen.

Kaiken kaikkiaan voidaan sanoa, että oikeanlainen nettikäyttäytyminen on paljon kiinni omista asenteista, mutta tiedon puutteet luovat paljon ongelmia. Pitkiin ja vaikeasti ymmärrettäviin rekisteriselosteisiin, joita ei tarjota omalla kielellä, ei jakseta tutustua. Seurausten ymmärtäminen pitäisi olla kaikilla tiedossa. Näin ei kuitenkaan selkeästi ole, koska sosiaaliset mediat tuovat

jatkuvasti lisää uusia ongelmia esille. Tulevaisuus tuo varmasti niitä vielä paljon lisää, myös uudenlaisissa muodoissa.

LÄHTEET

Alanko, H; Artte, U; Huhtala, H; Karonen, P; Koskiniemi,T; Kosunen, R; Lindén, T; Luhtala, R; Nissinen, V; Nordlund, A; Simell, T; Sukuvaara, H & Väyrynen, P. 2010. Sosiaalisen median sanasto, viitattu 28.3.11. http://www.tsk.fi/tiedostot/pdf/Sosiaalisen_median_sanasto.

Alexa 2011. twitter.com, viitattu 26.3.2011. http://www.alexa.com/siteinfo/twitter.com.

Carlson, N. 2010. At Last – The Full Story of How Facebook was founded, viitattu 26.3.2011. http://www.businessinsider.com/how-facebook-was-founded-2010-3#we-can-talk-about-that-after-i-get-all-the-basic-functionality-up-tomorrow-night-1.

Digitoday 2010. Varo Prisma-lahjakorttiarvontaa Facebookissa, viitattu 29.3.2011. http://www.digitoday.fi/tietoturva/2010/10/13/varo-prisma-lahjakorttiarvontaa-facebookissa/201014193/66.

Douglas, N. 2006. MySpace: The Business of Spam 2.0 (Exhaustive Edition) viitattu 26.3.2011. http://valleywag.gawker.com/tech/myspace/myspace-the-business-of-spam-20-exhaustive-edition-199924.php.

Facebook 2011a. Ohje- ja tukikeskus, viitattu 26.3.2011. http://www.facebook.com/help/?page=842.

Facebook 2011b. Facebook Security: Threats, viitattu 26.3.2011. http://www.facebook.com/security?v=app_4949752878/.

Guyhto, A. 2010. Five Reasons Not to Accept Facebook Friend Requests from Strangers, viitattu 26.3.2011. http://www.associatedcontent.com/article/5613196/five_reasons_not_to_accept_facebook.html?cat=41.

Harjuhahto-Madetoja, K; Aarnio R; Andersson, M; Elonen, R; Huuhtanen, J; Keronen, J; Kietäväinen, T; Korkeela, M; Markkula, M; Mattila, V-M; Repo, A. J; Rinne, K; Salminen, K; Silvennoinen, E; Sinkkonen, E; Suominen, R; Svento, R; Taipale, V; Turunen, V; Virmala, T; Viteli, J; Eskola, A; Honka, L. & Ahonen, V-V. 2006. Uudistuva, ihmisläheinen ja kilpailukykyinen Suomi, viitattu 27.3.2011. http://www.arjentietoyhteiskunta.fi/files/34/Kansallinen_tietoyhteiskuntastrategia.pdf.

Heikniemi, J. 2011. 140 merkin ihme, Mikrobitti 1/2011, 47-49.

Hintikka, K. A. 2007. Web 2.0 – johdatus internetin uusiin liiketoimintamahdollisuuksiin, viitattu 27.3.2011. http://www.tieke.fi/mp/db/file_library/x/IMG/20815/file/julkaisu_28.pdf.

Kangas, P; Toivonen, S; & Bäck, A. 2007. Googlen mainokset ja muita sosiaalisen median liiketoimintamalleja, viitattu 28.3.2011. http://www.vtt.fi/inf/pdf/tiedotteet/2007/T2369.pdf.

Koskinen, S. 2011. Sosiaalinen media voi vaikuttaa myös työsuhteisiin, Turun Sanomat 17.1.2011, 2.

Kotilainen, S. 2010. Vakuutusyhtiöt vaativat Facebook-sivuja todisteiksi, viitattu 29.3.2011. http://www.tietokone.fi/uutiset/vakuutusyhtiot_vaativat_facebook_sivuja_todisteiksi.

Leijel, M. 2010. How to permanently delete your facebook account, viitattu 26.3.2011. http://www.facebook.com/group.php?gid=16929680703.

Linnake, T. 2010a. Facebook säätää jälleen yksityisyysasetuksia, viitattu 26.3.2011. http://www.digitoday.fi/viihde/2010/10/07/facebook-saataa-jalleen-yksityisyysasetuksia/201013925/66.

Linnake, T. 2010b. Mark Zuckerberg sotkettiin mukaan Facebookin pedofiliapilaan, viitattu 26.3.2011. http://www.digitoday.fi/tietoturva/2010/10/10/mark-zuckerberg-sotkettiin-mukaan-facebookin-pedofiliapilaan/201014051/66.

Linnake, T. 2010c. Uhrit selviävät säikähdyksellä Facebookin suomihuijauksesta, viitattu 26.3.2011. http://www.digitoday.fi/yhteiskunta/2010/10/07/uhrit-selviavat-saikahdyksella-facebookin-suomihuijauksesta/201013905/66/.

Linnake, T. 2010d. 20 minuutin salasana luottaa liikaa käyttäjään, viitattu 26.3.2011. http://www.digitoday.fi/tietoturva/2010/10/14/20-minuutin-salasana-luottaa-liikaa-kayttajaan/201014300/66/.

Linnake, T. 2011. Facebookin uusi turva-asetus hämää, viitattu 26.3.2011. http://www.digitoday.fi/tietoturva/2011/02/24/facebookin-uusi-turva-asetus-hamaa/20112726/66.

Mediablogi 2008. Millainen on hyvä salasana?, viitattu 26.3.2011. http://hpguru.net/millainen-on-hyva-salasana/.

MySpace 2011a. Asetukset - Yksityisyys, viitattu 29.3.2011. http://www.myspace.com/my/settings/account/privacy.

MySpace 2011b. Selaa henkilöitä, viitattu 29.3.2011. http://www.myspace.com/browse/people.

MySpace 2011c. Omat jutut, viitattu 29.3.2011. http://www.myspace.com/guide/im.

Niiles, M. 2011. Työpaikan haukkuminen Facebookissa johtanut useisiin potkuihin, viitattu 26.3.2011. http://www.iltasanomat.fi/kotimaa/Ty%C3%B6paikan%20haukkuminen%20Facebookissa%20on%20johtanut%20useisiin%20potkuihin/art-1288361221616.html.

Owyang, J. 2008. Social Network Stats: Facebook, MySpace, Reunion, viitattu 26.3.2011. http://www.web-strategist.com/blog/2008/01/09/social-network-stats-facebook-myspace-reunion-jan-2008/.

Pitkänen, P. 2010a. F-Secure antaa 7 neuvoa Facebook-turvallisuuteen, viitattu 26.3.2011. http://www.digitoday.fi/tietoturva/2010/08/06/f-secure-antaa-7-neuvoa-facebook-turvallisuuteen/201010862/66.

Pitkänen, P. 2010b. Suomalainen Facebook-mato ryövää kännykkälaskulla, viitattu 26.3.2011. http://www.digitoday.fi/tietoturva/2010/09/07/mato-tunki-sisaan-facebookin-porsaanreiasta/201012356/66/.

Pitkänen, P. 2010c. Virkamiehiä varoitetaan ”hölmöilystä” nettiyhteisöissä, viitattu 26.3.2011. http://www.digitoday.fi/yhteiskunta/2010/12/27/virkamiehia-varoitetaan-holmoilysta-nettiyhteisoissa/201017925/66.

Pitkänen, P. 2011a. Facebook sulkee päivittäin alaikäisten sivuja, viitattu 26.3.2011. http://www.digitoday.fi/yhteiskunta/2011/03/24/facebook-sulkee-paivittain-alaikaisten-sivuja/20114157/66.

Pitkänen, P. 2011b. Facebook uusii profiilisivut väkisin – Näin suojaudut, viitattu 26.3.2011. http://www.digitoday.fi/tietoturva/2011/01/11/facebook-uusii-profiilisivut-vakisin---nain-suojaudut/2011396/66.

Pitkänen, P. 2011c. Facebook avaa uuden palvelun Suomessa - tarkista yksityisyysasetukset, viitattu 26.3.2011. http://www.digitoday.fi/tietoturva/2011/03/02/facebook-avaa-uuden-palvelun-suomessa---tarkista-yksityisyysasetukset/20112989/66.

Reinikainen, P. 2011. Varo tätä sovellusta Facebookissa, viitattu 26.3.2011. http://www.iltalehti.fi/digi/2011012113041159_du.shtml.

Reuters 2007. MySpacessa luultua enemmän seksuaalirikoksia, viitattu 27.3.2011. www.yle.fi/uutiset/ulkomaat/2007/07/myspacessa_luultua_enemman_seksuaalirikollisia_245228.html.

Rosendahl, M. 2002. Tietoturva kuuluu kaikille, viitattu 26.3.2011. http://www.helsinki.fi/atk/lehdet/402/Tietoturva_kuuluu_kaikille.html.

Sagolla, D. 2009. How Twitter Was Born, viitattu 26.3.2011. http://www.140characters.com/2009/01/30/how-twitter-was-born/.

Schonfeld, E. 2010. Costolo: Twitter Now Has 190 Million Users Tweeting 65 Million Times A Day, viitattu 26,3,2011. http://techcrunch.com/2010/06/08/twitter-190-million-users/.

Schram, K. 2010. Game Store Takes Souls Via EULA [April Fool's Fine Print Nets English Game Store The Souls Of 7000 Customers], viitattu 30.3.2011. http://nexus404.com/Blog/2010/04/16/game-store-takes-souls-via-eula-april-fools-fine-print-nets-english-game-store-the-souls-of-7000-customers/.

Smith, C. & Bosker, B. 2011. What NOT To Post On Facebook: 13 Things You Shouldn't Tell Your Facebook Friends, viitattu 26.3.2011. http://www.huffingtonpost.com/2010/11/01/what-not-to-post-on-facebook_n_764338.html#s157112&title=Your_Birth_Date.

Tampereen yliopisto tiedote 2007. Sosiaalisen median tekijänoikeuskysymyksistä ensimmäinen opas yrityksille, viitattu 26.10.2010. http://www.uta.fi/ajankohtaista2/tiedotteet/2007/5b.html.

Tietosuojavaltuutetun toimisto 2011. Tietosuoja turvaa oikeutesi, viitattu 26.3.2011. http://www.tietosuoja.fi/uploads/zg5sofwogs.pdf.

Unified Stream 2010. Facebook Reaches 600 Million Users and Bloomberg profiles Mark Zuckerberg, viitattu 26.3.2011. http://www.unifiedstream.com/facebook-reaches-600-million-users-bloomberg-profiles-mark-zuckerberg/.

Uusi Facebook-toiminto nosti myrskyn 2010. Ilta-Sanomat, viitattu 26.3.2011. http://www.iltasanomat.fi/ulkomaat/Uusi%20Facebook-toiminto%20nosti%20myrskyn/art-1288338681632.html.

Vaalisto, H. 2010. Facebook kehitti kertakäyttöisen salasanan, viitattu 26.3.2011. http://www.digitoday.fi/tietoturva/2010/10/13/facebook-kehitti-kertakayttoisen-salasanan/201014210/66/.

VAHTI Valtiovarainministeriö 2010. Sosiaalisen median tietoturvaohje, viitattu 26.3.2011. http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20101222Sosiaa/Sosiaalinen_media.pdf.

Vääräniemi, A. 2010. Facebookista voi nyt ostaa prepaid-kortilla, viitattu 26.3.2011. http://www.digitoday.fi/bisnes/2010/09/06/facebookista-voi-nyt-ostaa-prepaid-kortilla/201012302/66/.

Zuckerberg, M. 2010. 500 Million Stories, viitattu 26.3.2011. http://blog.facebook.com/blog.php?post=409753352130.